

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

Case No. 22 M 1000

The application seeks a warrant to search the apartment unit located at [REDACTED], the person of Minor A, and Electronic Devices (further described in Attachment A)

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Youstina Aziz, Special Agent with the US Immigration and Customs Enforcement Office of Homeland Security Investigations, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of Illinois, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is evidence, instrumentalities, and fruits.

The search is related to a violation of:

Code Section

Offense Description

Title 18, United States Code, Sections 2251(a); 2252A(a)(2)(A); and 2252A(a)(5)(B)

sexual exploitation of a child, receipt of child pornography, and possession of child pornography

The application is based on these facts:

See Attached Affidavit.

Continued on the attached sheet.



Applicant's Signature
YOUSTINA AZIZ, Special Agent
Homeland Security Investigations

Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: December 14, 2022

Judge's signature

City and State: Chicago, Illinois

GABRIEL A. FUENTES, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Youstina Aziz, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the US Immigration and Customs Enforcement Office of Homeland Security Investigations (“HSI”) and have been so employed since approximately September 2020. As such, I am an investigative or law enforcement officer of the United States empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516(1). Prior to my tenure as a Special Agent with HSI, I was a Deputy Sheriff with the Albany County Sheriff’s Office and a Police Officer with the Troy Police Department from approximately December 2018 until approximately September 2020. As part of my duties as a Special Agent with HSI, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have completed the HSI Special Agent Training program at the Federal Law Enforcement Training Center in Glynco, GA. During both basic training, and subsequent training, I received instruction on conducting online child pornography investigations. I have observed and reviewed numerous examples of child

pornography (as defined in 18 U.S.C. § 2256) in multiple forms of media, including computer media. I have also been the affiant for several federal search warrants to include warrants for residential and online account searches and participated in the execution of federal search warrants involving child pornography and child-exploitation investigations.

2. This affidavit is made in support of an application for a warrant to search the following: (A) the residence located [REDACTED] [REDACTED] (the “Subject Premises” as more particularly described in Attachment A), (B) the person of Minor A,¹ and (C) any computers, computer equipment, or computer storage media and electronic storage media (including cellular telephones) (collectively, the “Electronic Devices”) located during the searches of the Subject Premises or Minor A’s person, provided such Electronic Device is found either on Minor A’s person, in what the executing officials reasonably believe to be Minor A’s bedroom, or in any common area of the Subject Premises if the executing officials reasonably believe that the Electronic Device found in a common area belongs to or is regularly used by Minor A for evidence, fruits, and instrumentalities relating to violations of Title 18, United States Code, Sections 2251(a) (sexual exploitation of a child), 2252A(a)(2)(A) (receipt of child pornography), and 2252A(a)(5)(B) (possession

¹ Minor A is a minor female believed to be 16 years old.

of child pornography) (the “**Subject Offenses**”), as more fully described in Attachment B.²

3. The statements in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found during searches of the Subject Premises, the person of Minor A, and the Electronic Devices found therein and thereon, as discussed further below.

II. **PROBABLE CAUSE**

The Arrest of [REDACTED] and the Underlying Investigation

4. On or about December 6, 2022, the United States District Court for the [REDACTED] found probable cause to charge [REDACTED] with receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A) by criminal complaint. A copy of the complaint and affidavit is attached here as **Exhibit 1** and incorporated herein by reference. Prior to that arrest, the same Court found probable cause to issue search warrants for, among other things, certain Google Accounts

² Electronic Devices does not include devices in bedrooms of occupants of the Subject Premises other than Minor A or the personal cellular telephones of individuals other than Minor A.

linked to [REDACTED] and [REDACTED] residence and Electronic Devices. *See Exhibit 2 and Exhibit 3*, which also are incorporated herein by reference.

5. As set forth in more detail in **Exhibits 1-3**, [REDACTED] has been interacting with multiple minor females online, asking them to create sexually explicit material of themselves, and watching livestreams and receiving video files depicting the sexually explicit conduct.³ Based on the information set forth in more detail in **Exhibit 2** and **Exhibit 3** and as discussed further below, [REDACTED] was working with Minor A to convince other, younger female children to create the sexually explicit material for [REDACTED]. Among other things, Minor A appears (clothed) in one of the child pornography videos recovered during the investigation. That video shows Minor A, [REDACTED], and a naked minor victim who displays her vagina to the camera and is seen communicating with both [REDACTED] and Minor A. In addition, IP connection records for one of the Google Accounts that was the subject of the search warrant application in **Exhibit 2** shows that it was logged into from the Subject Premises (Minor A's residence) during times when child pornography files were uploaded to the account, and the internet service for that IP address is subscribed to by Minor A's mother.

[REDACTED]

6. [REDACTED]

[REDACTED]

³ The child pornography files described in **Exhibits 1-3** are available for review by this Court upon request.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

7.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4

[REDACTED]

5

[REDACTED]

[REDACTED]

[REDACTED]

8. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁶ [REDACTED]

c) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

9. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

10. [REDACTED]

[REDACTED] records obtained during the investigation, including child pornography files found in the Google Accounts referred to in **Exhibit 2** (including one with Minor A's face visible), IP and internet subscriber records that

resolve to the Subject Premises, and information about Minor A's age, birthday, and physical residence that [REDACTED] knew and conveyed during the proffer session.

*Information Linking Minor A to the Subject Premises
and More Recent Activity Involving Child Exploitation Material*

11. On or about November 2, 2022, Special Agent James Hamilton with HSI served an administrative summons to T-Mobile seeking subscriber information for IP address 2607:fb90:e1bf:bb02:2da6:9a1b:5d0e:140e, which was used based on information provided by Google in a CyberTip at various times on or about September 3, 2022, to login into the Google account [REDACTED]@gmail.com.⁷ The summons also requested subscriber records for IP addresses 2607:fb90:a3a2:f8ae:41ac:c786:12ba:7466, 2607:fb90:264:16a0:d992:23e:fabd:a3ad, 2607:fb90:e138:4607:7bbe:846c:9805:f867, which were also used (according to Google CyberTip information) at various times during which child pornography files were uploaded to the Google account.

12. On or about November 7, 2022, T-Mobile responded that these IP addresses were assigned to Minor A's mother at the Subject Premises (the apartment number was not provided, but the street address matches the address for the Subject

⁷ This account associates to Minor A through [REDACTED] proffer statement, username, and subscriber records (as reflected further below).

Premises). The subscriber information also listed multiple telephone numbers, one of which was associated with the Google Account identified above.

13. On or about December 9, 2022, I received information from the Chicago Police Department that Minor A is a student at a local public high school with a listed address at the Subject Premises (without the apartment number identified). The Chicago Police Department also had access to records from the school reflecting Minor A's mother's name, which matches the name of the subscriber records discussed above. On or about the same day, a query of law enforcement and immigration databases reflected that Minor A's parents listed the Subject Premises as their residence, including Unit "████" The address information also is consistent with information obtained from the Chicago Department of Children and Family Services, received on or about the same day, which identified the same the same address and Unit Number █████(without the "████" at the end).

III. BACKGROUND INFORMATION CONCERNING CHILD PORNOGRAPHY

14. Based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers affect the methods used by people who possess, receive, distribute, and transport child pornography in these ways:

15. Those who create child pornography can produce both still and moving images directly from a common video or digital camera, and other devices that create

video and still images, including most cellular telephones and Personal Digital Assistants (“PDA”) (e.g., a Blackberry). Images from such devices can be transferred to a computer by attaching the device to the computer using a cable, or by uploading images from the device’s memory card directly onto the computer or into a storage account accessible from any computer with the capability of accessing the internet (sometimes referred to as a “cloud” account). Once on the computer, images can then be stored, manipulated, transferred, or printed. This includes transfer to some of the same types of devices that are commonly used to create child pornography, such as cellular telephones and PDAs, as well as other computers. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography.

16. The Internet allows any computer to connect to another computer. Electronic contact can be made to millions of computers around the world. The Internet allows users, while still maintaining anonymity, to locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. They can also distribute and collect child pornography with peer-to-peer (“P2P”) file sharing, which uses software to link computers together through the Internet to form a network that allows for the sharing of digital files among users on the network. These communication links allow contacts around the world as easily as calling next

door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet.

17. The computer's capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise, optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media, such as floppy disks, also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child pornography search warrants often find electronic, optical, and/or electromagnetic storage media containing child pornography in the same location as or near the computer that was used to obtain, access, and/or store child pornography.

18. My training and experience, and the training and experience of other agents whom I have consulted, have shown the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of

photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or other images, as well as literature describing sexually explicit activity involving children. Such individuals frequently store their child pornography on multiple electronic, optical, and/or electromagnetic storage media, including not only their computer, but also on external hard drives, floppy disks, CD-ROMs, DVDs, memory sticks, thumb drives, cell phones, PDAs, and other such media. Many of these individuals also collect child erotica, which consist of items that may not rise to the level of child pornography but which nonetheless serve a sexual purpose involving children.

b. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, Internet Relay Chat, newsgroups, instant messaging, and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute child pornography often collect, read, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original

medium from which they were derived, in address books or notebooks, on computer storage devices, or merely on scraps of paper.

d. The majority of individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. These individuals almost always maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including filing cabinets, safes, or lockboxes. These individuals may also maintain their collections in password-protected or encrypted electronic media. They may keep these passwords, and other information concerning their use of the computer, on handwritten or printed notes that they store in personal areas and around the computer.

IV. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

19. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (e.g. computer hardware, computer software, computer related documentation, and cellular telephones) to be processed later by a

qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. To fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a

thorough and efficient search due to software and hardware configuration issues. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

21. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and are subject to seizure as such if they contain contraband or were used to obtain or store images of child pornography.

V. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

22. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

23. The review of electronically stored information and electronic storage media removed from the devices described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the Subject Offenses specified above;

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word searches of files, to determine whether their contents fall within the items to be seized as set forth in Attachment B.

24. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

VI. BIOMETRIC ACCESS TO DEVICES

25. The requested warrant would also permit law enforcement to compel Minor A to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and discussions with other law enforcement officers and HSI special agents, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a

more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience and discussions with other law enforcement officers, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric

features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

26. The proposed warrant does not authorize law enforcement to require Minor A to state or otherwise provide a password (or any other means that may be used to unlock or access the devices). Moreover, the proposed warrant does not authorize law enforcement to require Minor A to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

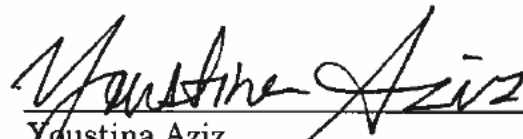
VII. LAW ENFORCEMENT AGENCIES ASSISTING HSI

27. This search warrant will be executed by your affiant and other HSI Special Agents, however, law enforcement officers from other agencies involved in this investigation, to include the [REDACTED] State Police and the Chicago Police Department may be utilized by HSI in the execution of this search warrant, to include the forensic examination of any electronic storage media devices that may be seized and later analyzed at a computer forensic laboratory.

VIII. CONCLUSION

28. Based on the foregoing, your affiant respectfully submits that there is probable cause for the requested warrant.

FURTHER AFFIANT SAYETH NOT.



Youstina Aziz
Special Agent
Homeland Security Investigations

Sworn to and affirmed by telephone 14th day of December, 2022

Honorable GABRIEL A. FUENTES
United States Magistrate District

ATTACHMENT A

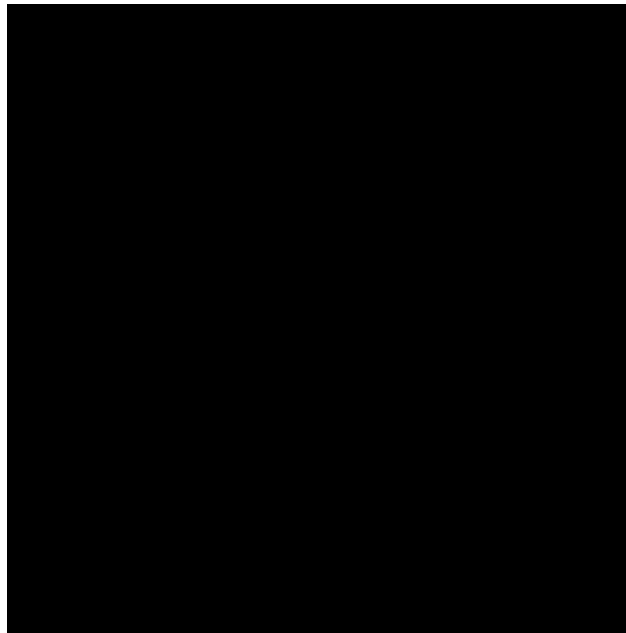
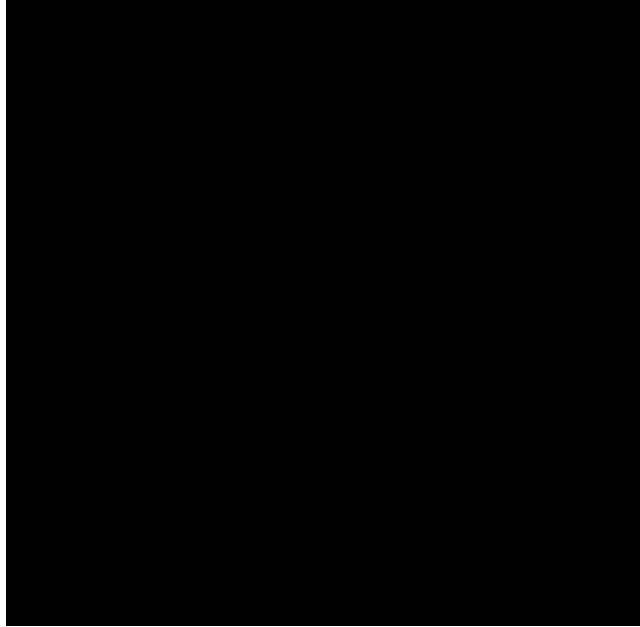
DESCRIPTION OF PREMISES, PERSON, AND ITEMS TO BE SEARCHED

The premises, person, and items to be searched are: (A) the apartment located at [REDACTED], to include all rooms, closed containers, and other places therein (the “Subject Premises”), (B) the person of Minor A, and (C) any computers, computer equipment, or computer storage media and electronic storage media (including cellular telephones) (collectively, the “Electronic Devices”) located during the searches of the Subject Premises or Minor A’s person, provided such Electronic Device is found either on Minor A’s person, in what the executing officials reasonably believe to be Minor A’s bedroom, or in any common area of the Subject Premises if the executing officials reasonably believe that the Electronic Device found in a common area belongs to or is regularly used by Minor A.

The exterior of the building containing the Subject Premises is depicted below and is further described as a yellow brick apartment building, labeled “[REDACTED]” on the front door.



The person of Minor A is depicted below:



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Fruits, evidence, contraband, and instrumentalities of violations of 18 U.S.C. § 2251(a), 18 U.S.C. § 2252A(a)(2)(A), and 18 U.S.C. § 2252A(a)(5)(B) (the “Subject Offenses”), as follows:

1. Items, documents, or digital files in any format and medium pertaining to the sexual exploitation of children, or to the possession, receipt, production, or distribution of child pornography as defined in 18 U.S.C. § 2256(8);
2. In any format and medium, originals, computer files, and copies of child pornography as defined in 18 U.S.C. § 2256(8);
3. Items, documents and computer files in any format and medium concerning minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
4. Documents in any format or medium that describe or refer to online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, user logins and passwords for such online storage or remote computer storage, including but not limited to Dropbox and iCloud;

5. Documents, digital files, or other items reflecting the use of file-sharing technology (not to include contents of files shared that are not otherwise within the scope of this attachment);

6. Items in any format or medium that describe or refer to any accounts belonging to or used by Minor A or [REDACTED] with an Internet Service Provider;

7. Documents or other items demonstrating the attachment of other computer hardware or storage media;

8. Passwords, encryption keys, and other access devices that may be necessary to access the electronic devices;

9. Counter forensic programs and associated data that are designed to eliminate data, including documents or other items demonstrating counter forensic programs and associated data that are designed to eliminate data;

10. Items in any format and medium depicting a relationship between [REDACTED], Minor A, and other minors that pertain to the engagement of illegal sexual activity or Subject Offenses;

11. Any items that can be used to identify minor children that have at any time been in [REDACTED] care;

12. Documents or computer files in any format or medium, or other items, that demonstrate the use, ownership, or control of the electronic devices, including the times the device was accessed, such as sales receipts, bills for Internet access, and notes;

13. Records evidencing who resides at the Subject Premises identified in Attachment A and who had/has access and/or was staying at the premises and records concerning ownership and/or control of any Electronic Device(s) associated with Minor A found within the premises identified in Attachment A;

14. Records concerning ownership and/or control of any Electronic Device(s) found on Minor A's person;

15. Records evidencing who accessed any internet connection at the premises identified in Attachment A and with what device(s) concerning the sexual exploitation of a child and/or the receipt/possession of any visual depictions of children engaged in sexually explicit conduct;

16. Records concerning use, ownership, and/or control of the following Google accounts: [REDACTED]@gmail.com, [REDACTED]@gmail.com, [REDACTED]@gmail.com, [REDACTED]@gmail.com;

17. Records of any passwords, passcodes, electronic keys, encryption codes, or any other electronic record for the purpose of using such record to gain access to all or part of the data on an electronic device authorized to be seized and searched pursuant to this warrant.

Photographs of Search

18. During the searches of the location and person set forth in Attachment A, photographs may be taken to record the condition thereof and/or the location of items found therein or thereon.

Biometric Access to Electronic Devices

19. During the execution of the searches of the location and person described in Attachment A, investigators are authorized to (1) press or swipe the fingers (including thumbs) of Minor A to the fingerprint scanner of any seized device(s) for the purpose of unlocking the device(s) to effectuate the authorized search; and (2) hold any seized device(s) in front of Minor A's face to activate the facial recognition and/or iris recognition feature of the device(s) for the purpose of unlocking the device(s) to effectuate the authorized search.

*Law Enforcement Agencies
Participating in the Search of the Residence and Items Seized*

20. Homeland Security Investigations (HSI) and other law enforcement agencies in [REDACTED] and Illinois will execute this search warrant and conduct forensic previews of electronic evidence at the search warrant scene. Additionally, seized electronic evidence will be examined at computer forensic laboratories operated by one or more of these agencies.

ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information, including cell phones, that are described in Attachment B and found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant.

Subject to the exceptions to the warrant requirement as recognized by law, the government may search only those electronic storage media that fall within the criteria as described in Attachment B, which may either be all electronic storage media found in the premises or only a subset of the electronic storage media found in the premises.

The government's review of removed electronic storage media shall be conducted pursuant to the following protocol:

The government must make reasonable efforts to use methods and procedures that will locate those categories of data, files, documents, or other electronically stored information that are identified in the warrant, while minimizing exposure or examination of categories that will not reveal the items to be seized in Attachment B.

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures if those procedures are designed to minimize the review of information not within the list of items to be seized as set forth in Attachment B:

a. examination of categories of data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;

c. surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word or concept searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B; and

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment B.

Law enforcement personnel are not authorized to conduct additional searches for any information beyond the scope of the items to be seized by this warrant as set forth in Attachment B. To the extent that evidence of crimes not within the scope of this warrant appears in plain view during the government's review, the government shall submit a new search warrant application seeking authority to expand the scope of the search prior to searching portions of that data or other item that is not within the scope of the warrant. However, the government may continue its search of that

same data or other item if it also contains evidence of crimes within the scope of this warrant.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

Exhibit 1

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

UNITED STATES OF AMERICA

v.

Case No. 1:22-md-765-SS

Defendant.

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of October 2021 through December 2022 in the county of [REDACTED] in the [REDACTED]

[REDACTED] the defendant violated:

Code Section

18 U.S.C. § 2252A(a)(2)(A)

Offense Description

Receipt of child pornography

This criminal complaint is based on these facts:
See Attached Affidavit

☒ Continued on the attached sheet.



Complainant's signature

Youstina Aziz, HSI Special Agent

Printed name and title

Attested to by the affiant in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Date: 12/6/2022



Judge's signature

City and State: [REDACTED]

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Youstina Aziz, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the US Immigration and Customs Enforcement Office of Homeland Security Investigations (“HSI”) and have been since September 2020. As such I am an investigative or law enforcement officer of the United States empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516(1). Prior to my tenure as a Special Agent with HSI, I was a Deputy Sheriff with the [REDACTED] Sheriff’s Office and a Police Officer with the [REDACTED] Police Department from December 2018 until September 2020. I have completed the HSI Special Agent Training program at the Federal Law Enforcement Training Center in Glynco, GA. During both basic training, and subsequent training, I received instruction on conducting online child pornography investigations. I have also been the affiant for several Federal search warrants to include warrants for residential and online account searches and participated in the execution of Federal search warrants involving child pornography and child exploitation investigations.

2. I have been investigating [REDACTED] for violating, *inter alia*, 18 U.S.C. § 2252A(a)(2)(A) (receipt of child pornography) (the “Subject Offense”). I submit this affidavit in support of a criminal complaint charging [REDACTED] with the Subject Offense.

3. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from others during my participation in this investigation, including other law enforcement officers, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described here, and information gained through my training and experience. This affidavit does not set forth everything I know about this

investigation because it is submitted for the limited purpose of securing a criminal complaint charging [REDACTED] with the Subject Offense.

PROBABLE CAUSE

4. In May 2022, the [REDACTED] Police Department (“UAPD”) responded to a police complaint from the mother of an 11-year-old girl (V1) who reported that her daughter had been contacted online by an unknown individual who solicited sexually explicit photos of the daughter’s “private areas.” According to V1’s mother and V1, someone had threatened V1 on a social media application, saying that he would come to her house and rape her if she did not send him the photos/videos he requested. V1 also reported that, between approximately October 2021 and February 2022, she created and sent sexually explicit images and videos of herself to that person.

5. [REDACTED] obtained [REDACTED] state search warrants for the target’s social media account. [REDACTED] identified [REDACTED] as the person likely using that account because it was accessed by IP addresses that return to Verizon and T-Mobile cell phone accounts registered to [REDACTED]

6. Among other things, the account contained a video file comprised of child sexual abuse material (CSAM) that depicted V1, identified by the state investigator who interviewed her and by the background of the video which matches V1’s bedroom. The file is described as follows:

- a. Filename: unified_message12499554085498065 is a one minute and 28 second video depicting a prepubescent female, who appears to be approximately 11 years old, that is naked, and squatting in front of a camera. The female subject’s fingers are in or around her vaginal area while she rubs her vagina. The female child’s vagina is visible to the camera in the video.

7. In October 2022, HSI learned of several CyberTips submitted to the National Center for Missing and Exploited Children which also associated to [REDACTED]. Among other things, his cellular telephone number related to three of the four accounts identified in the CyberTips. Multiple files in the accounts and included with the CyberTips were CSAM. Among other files,

the first file described below was found in one of the accounts and the second was included in one of the CyberTip reports:

- a. screen-20220428-000032-1hvlxfkg04d47.mp4 – This video file is 1 minute and 10 seconds long. It starts by depicting three video screens, including one depicting [REDACTED] whose face is visible, an unknown female, and a nude female child (V2) aged approximately 8-10 years old. During the video, V2 moves closer to the camera so the focus of the video is on her vagina [REDACTED] camera is then turned off, and the videos are reorganized spatially so that unknown female's head is depicted on top of V2's body.
- b. Google-CT-RPT-c7984a98d01be88aa31c724f103e26b6-VID-20220406-WA002.mp4 – This video file is 1 minute and 41 seconds long. It depicts three individuals on a video chat. One of the individuals is [REDACTED] The two other individuals are prepubescent minor female children who appear approximately 10-12 years old (V3 and V4). One of the minors asks if they “can just do pants?” and “do we do it with our shirt on?” [REDACTED] shakes his finger to indicate “no.” The other female child states, “no clothes bro.” V3 and V4 then sit naked on the floor, and [REDACTED] gestures for them to spread their legs. He gives a ‘thumbs up’ and V3 and V4 urinate on the floor.

8. On December 6, 2022, HSI and other law enforcement agencies executed a search warrant at [REDACTED] residence. HSI recovered an iPhone 6s cellular telephone that [REDACTED] provided the passcode to. Within a social media and messaging application, investigators saw a chat log with V3's name. Within that log is a 7 minute and 44 second video file, apparently received on December 2, 2022, at approximately 9:13 p.m. depicting V3 inserting an electronic toothbrush into her vagina. The photos application for the phone also contained a “Hidden” album with multiple child pornography videos, including the following:

- a. Filename: d51ee140-262d-443c-b879-d614244fc3e9, Dated: 11/15/2022-10:40 PM. This is a 27 second video depicting a pubescent minor that appears to be 12-15 years old. The minor is naked and on a floor in a ‘crab-like’ position. Her feet and hands are on the floor and her body is elevated. Her legs are spread, exposing her vagina to the camera. Approximately 13

seconds into the video, the minor looks at her vaginal area and begins to urinate on the floor.¹

9. In connection with the execution of the search warrant, [REDACTED] was interviewed after being provided his *Miranda* warnings, and that interview was recorded. Among other things, [REDACTED] admitted that he had an online friend with V3's name.

CONCLUSION

10. Based on the information above, there is probable cause to believe that [REDACTED] has violated 18 U.S.C. § 2252A(a)(2)(A) (receipt of child pornography), and I request a criminal complaint be issued pursuant to that violation of federal law.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

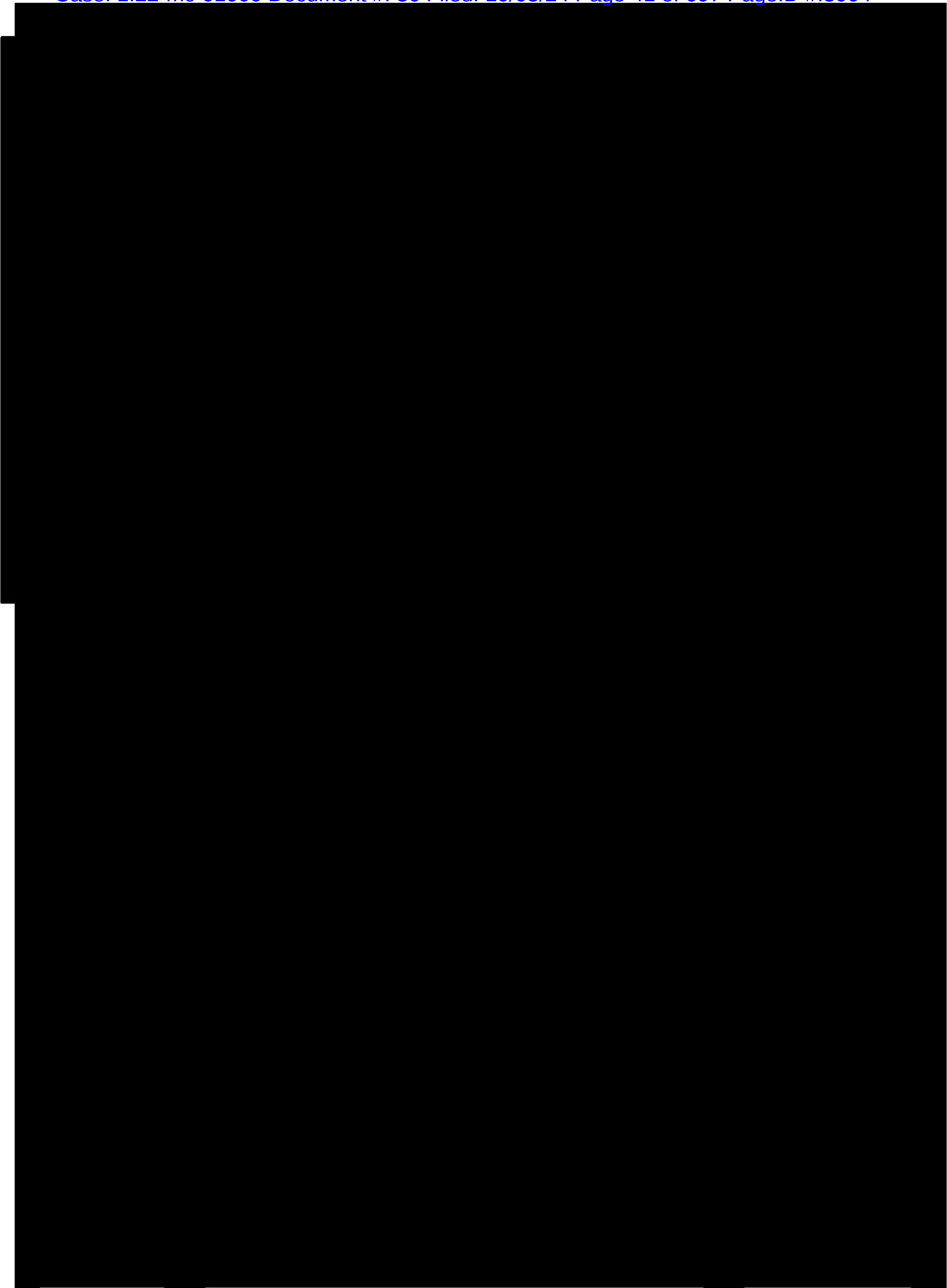

Youstina Aziz
Special Agent
Homeland Security Investigations

I, the Honorable [REDACTED] United States Magistrate Judge, hereby acknowledge that this affidavit was attested to by the affiant ~~by telephone~~ on December 6, 2022, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.



¹ The CSAM material described in this affidavit is available for the Court's review upon request.

Exhibit 2



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

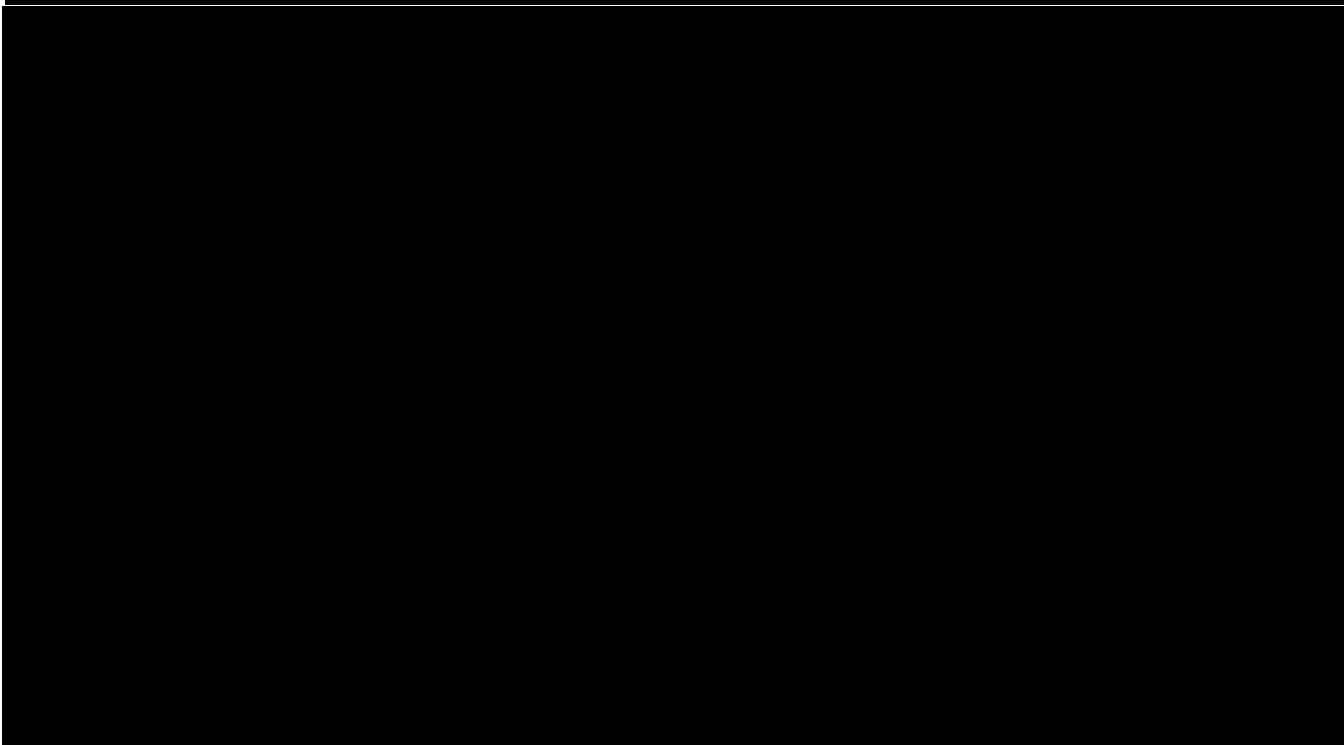
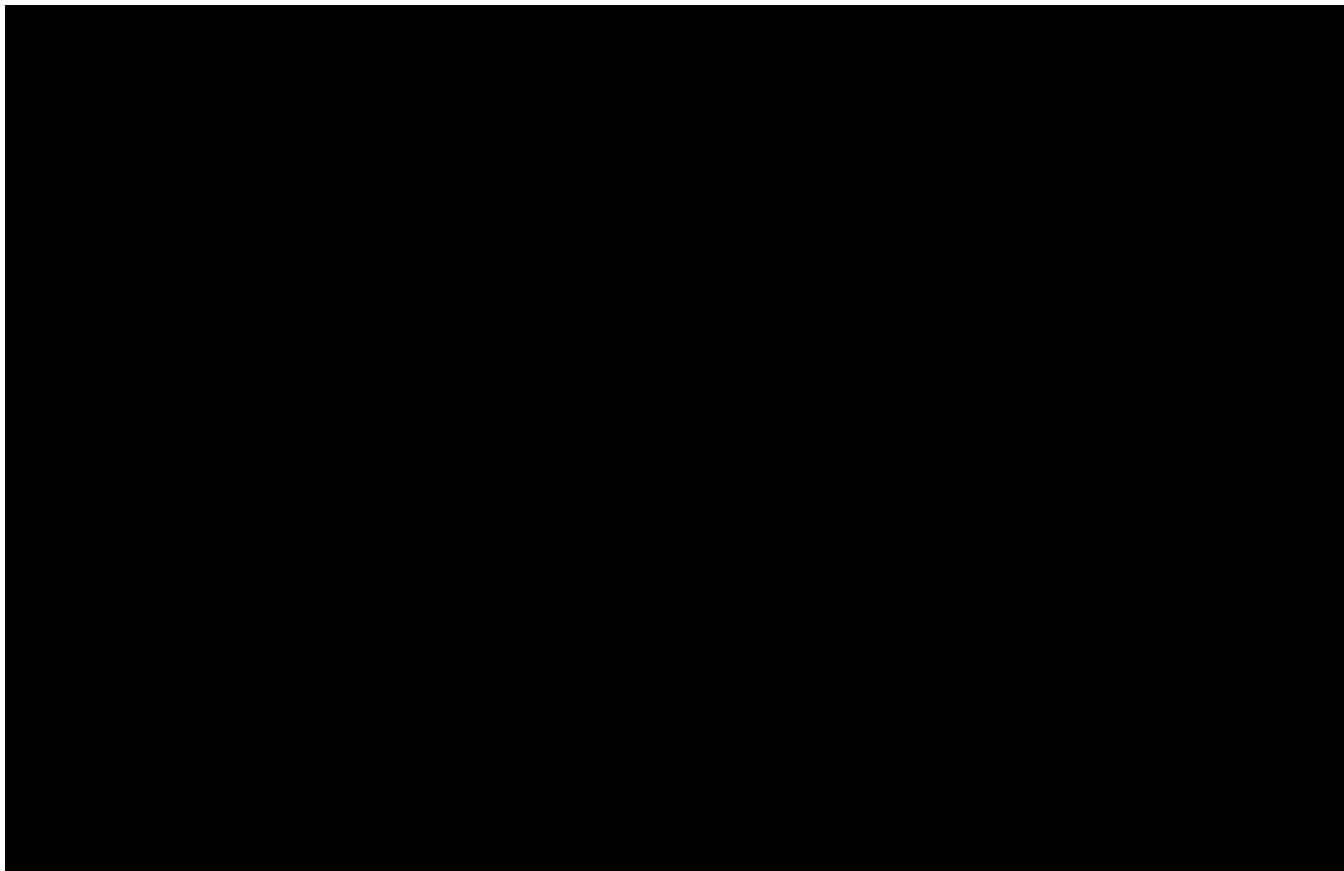
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

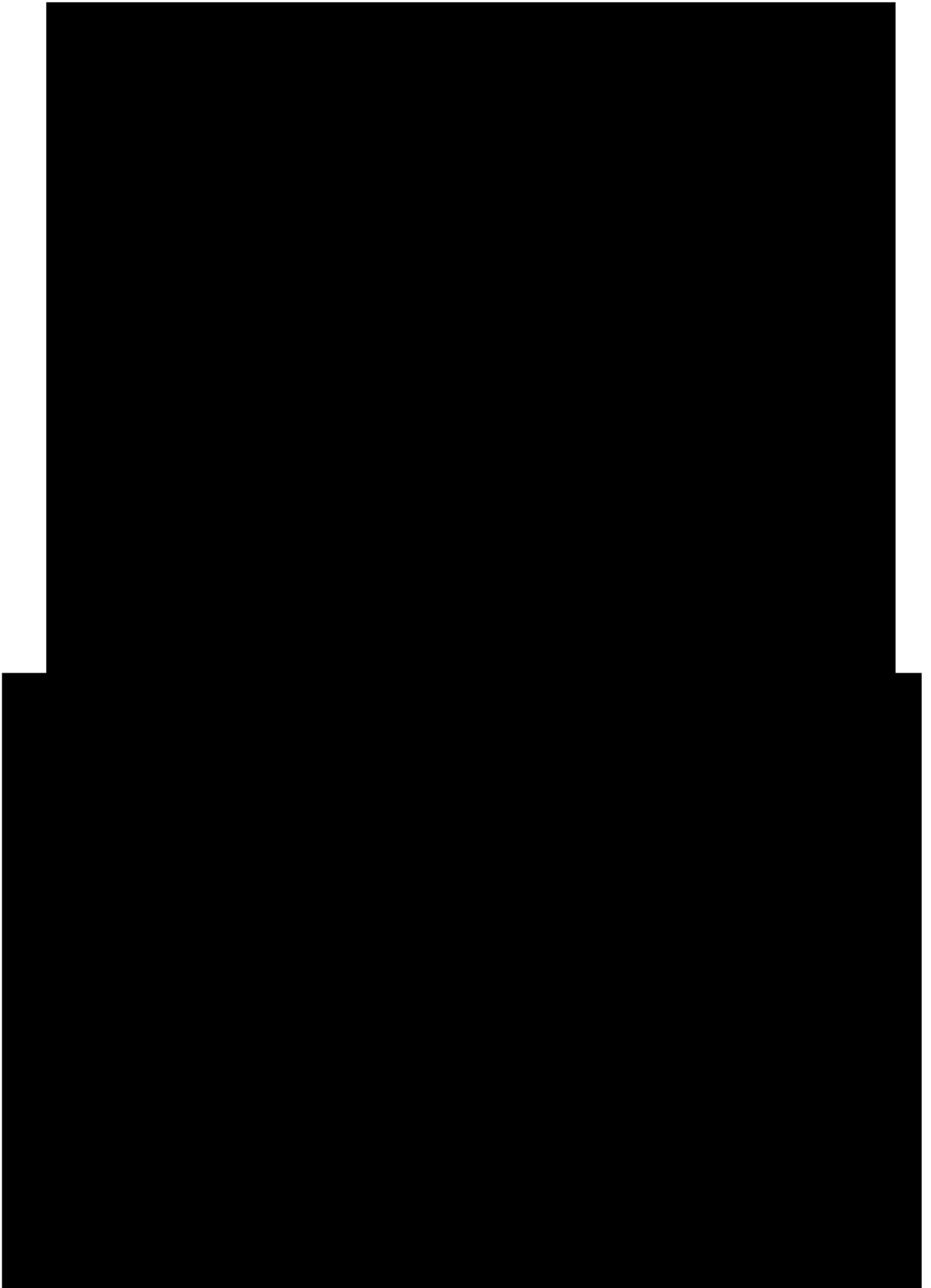
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

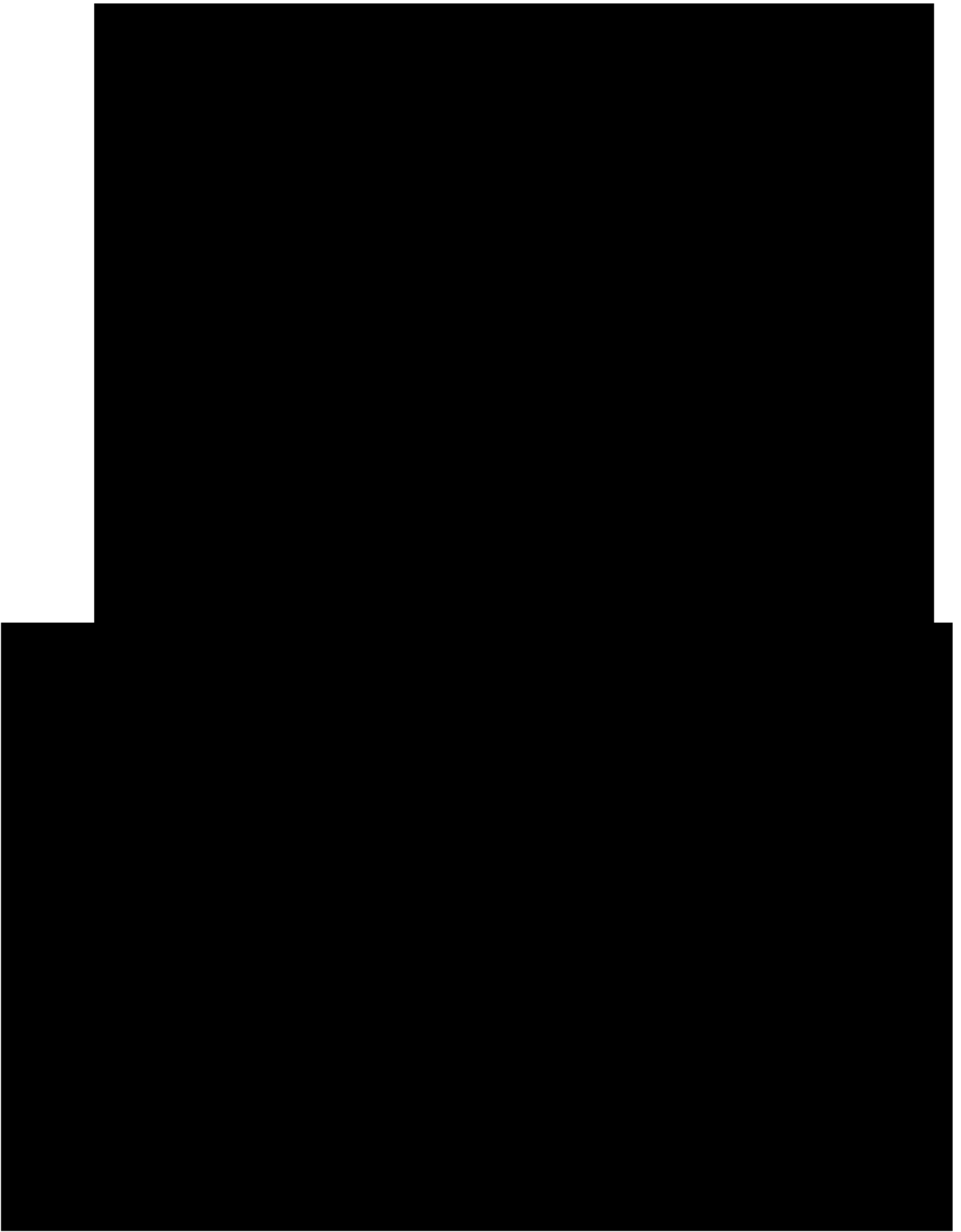
[REDACTED]

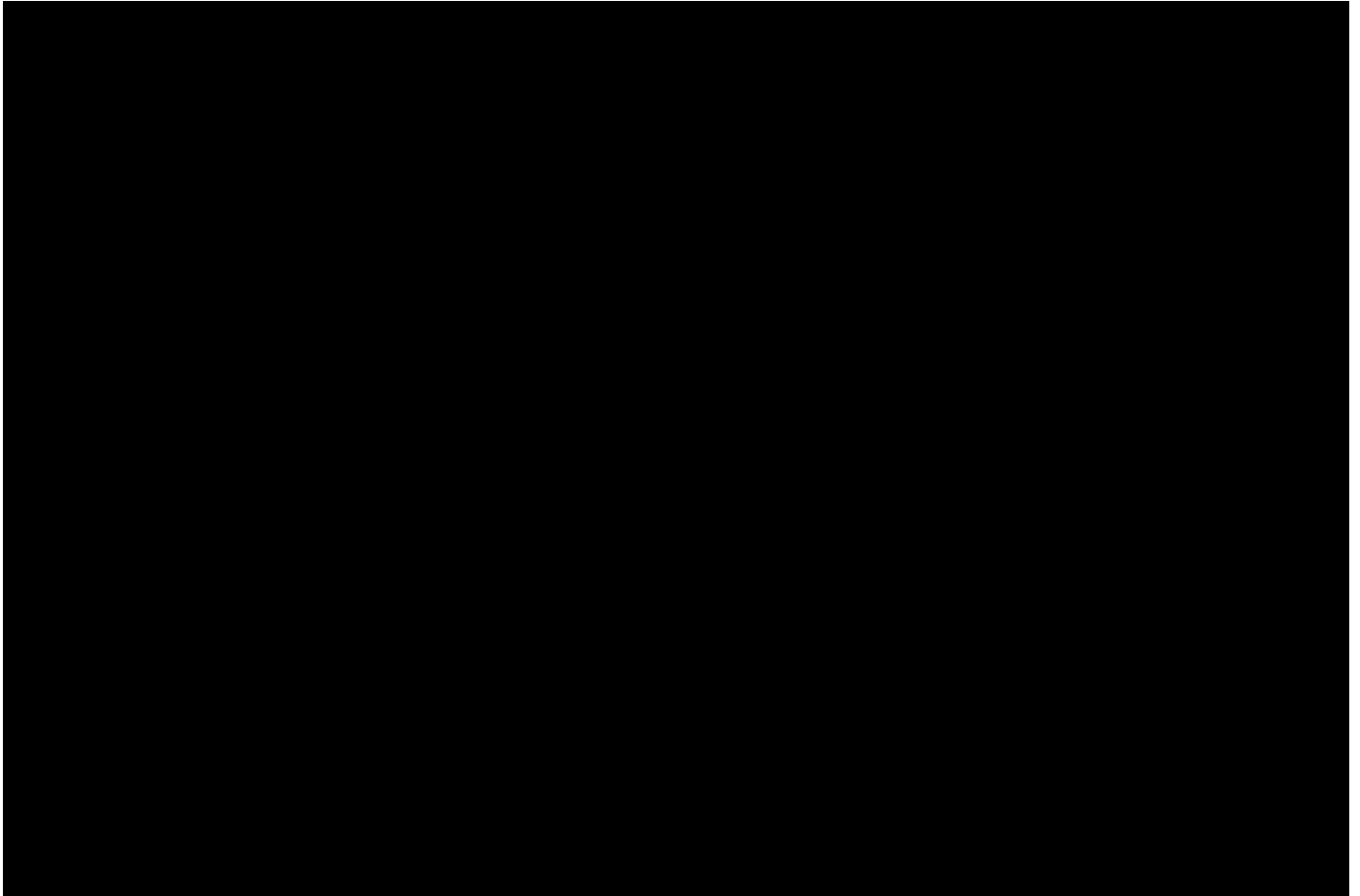
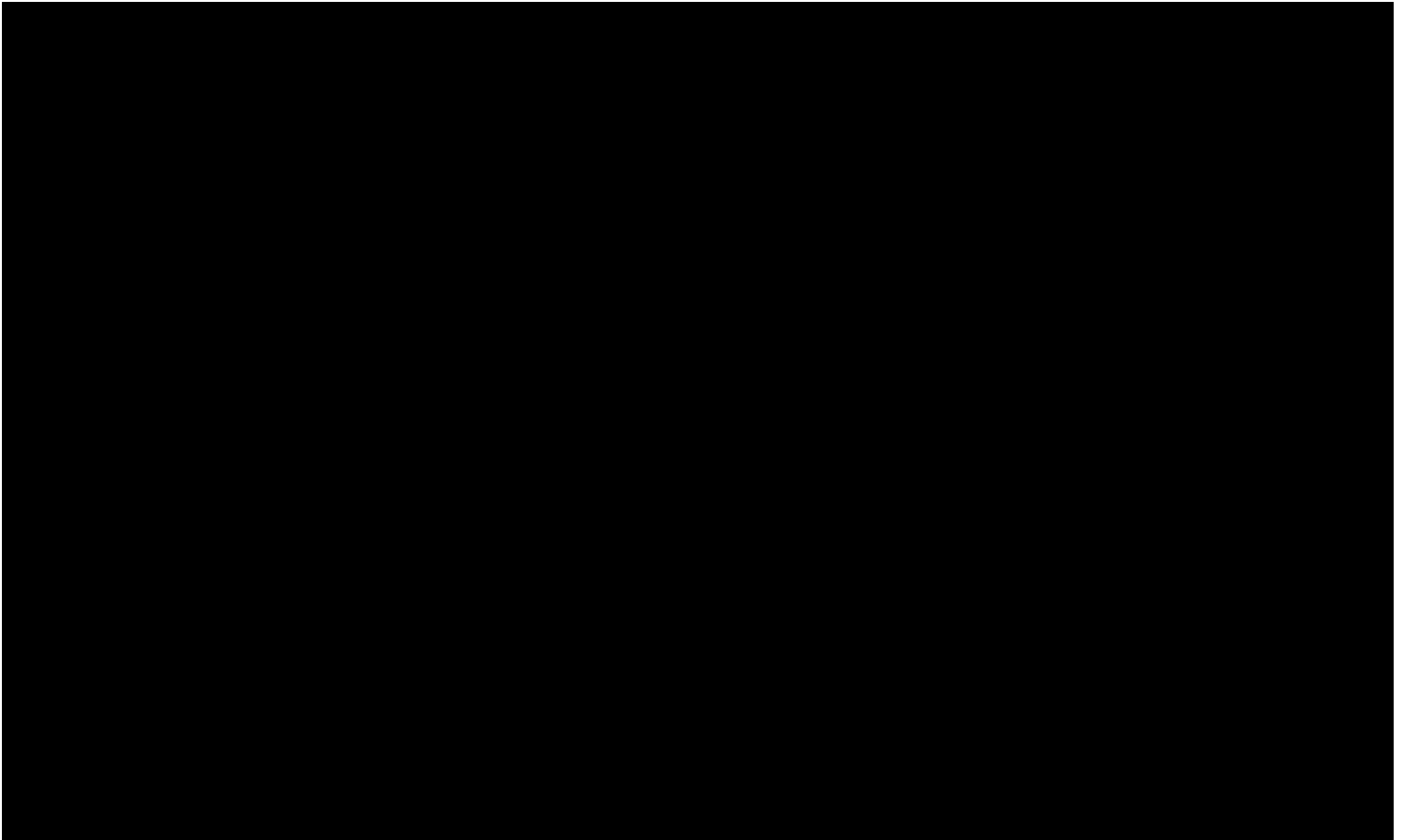


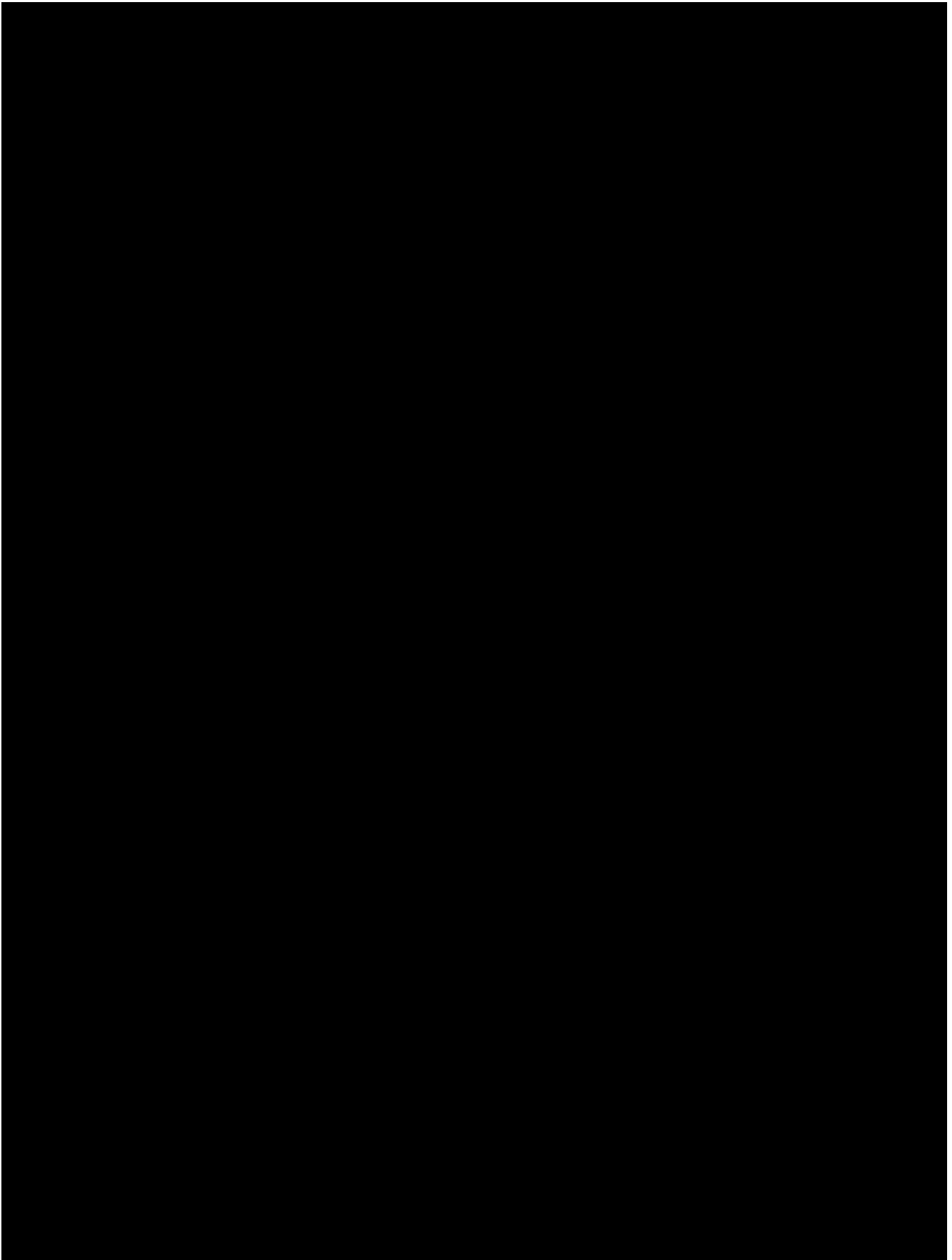
[REDACTED]

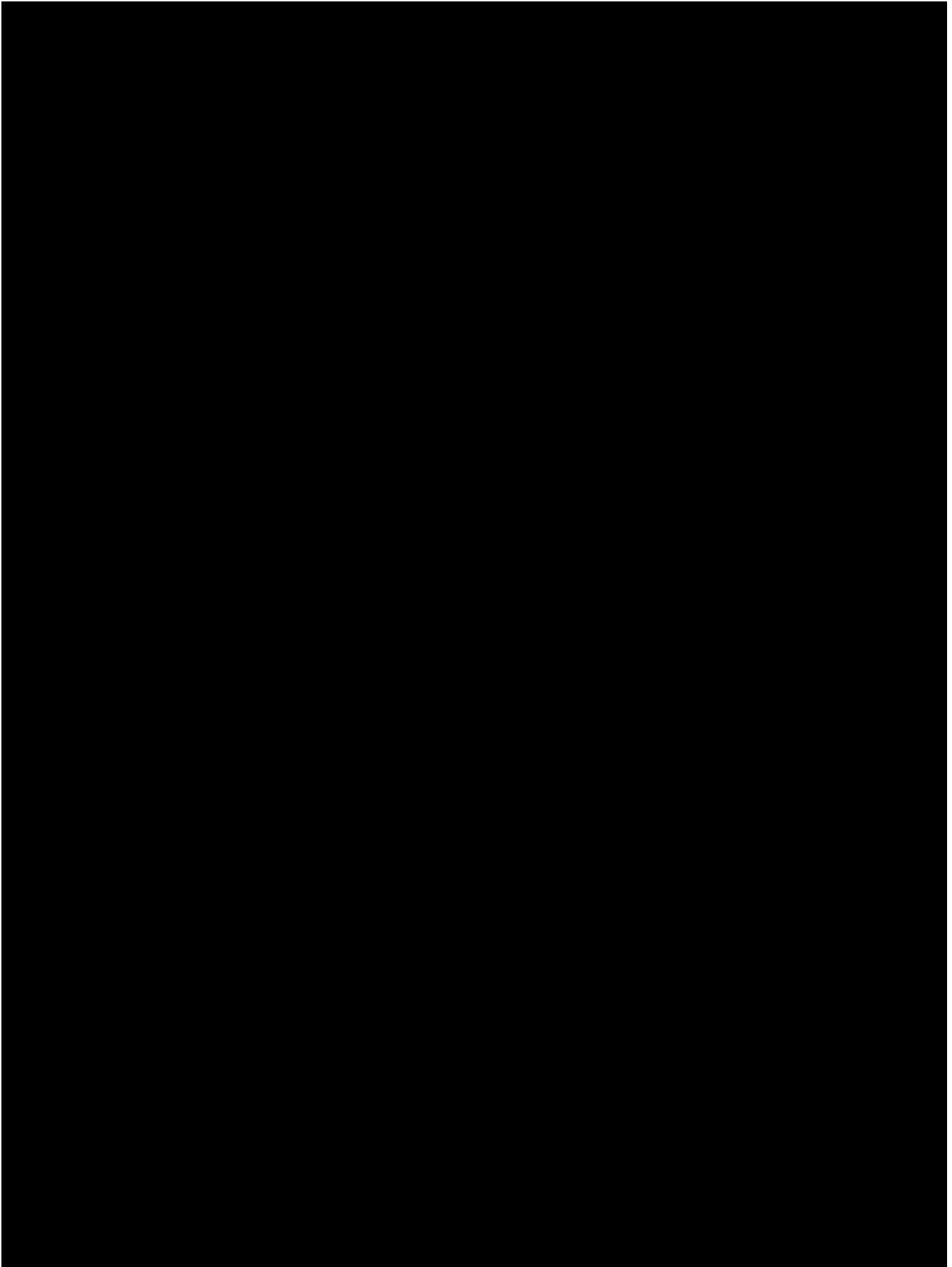
[REDACTED]

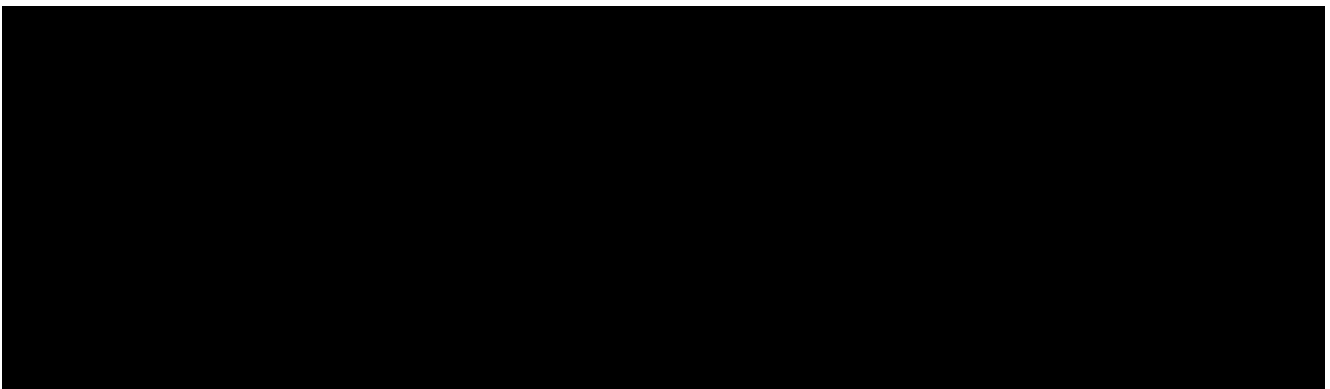
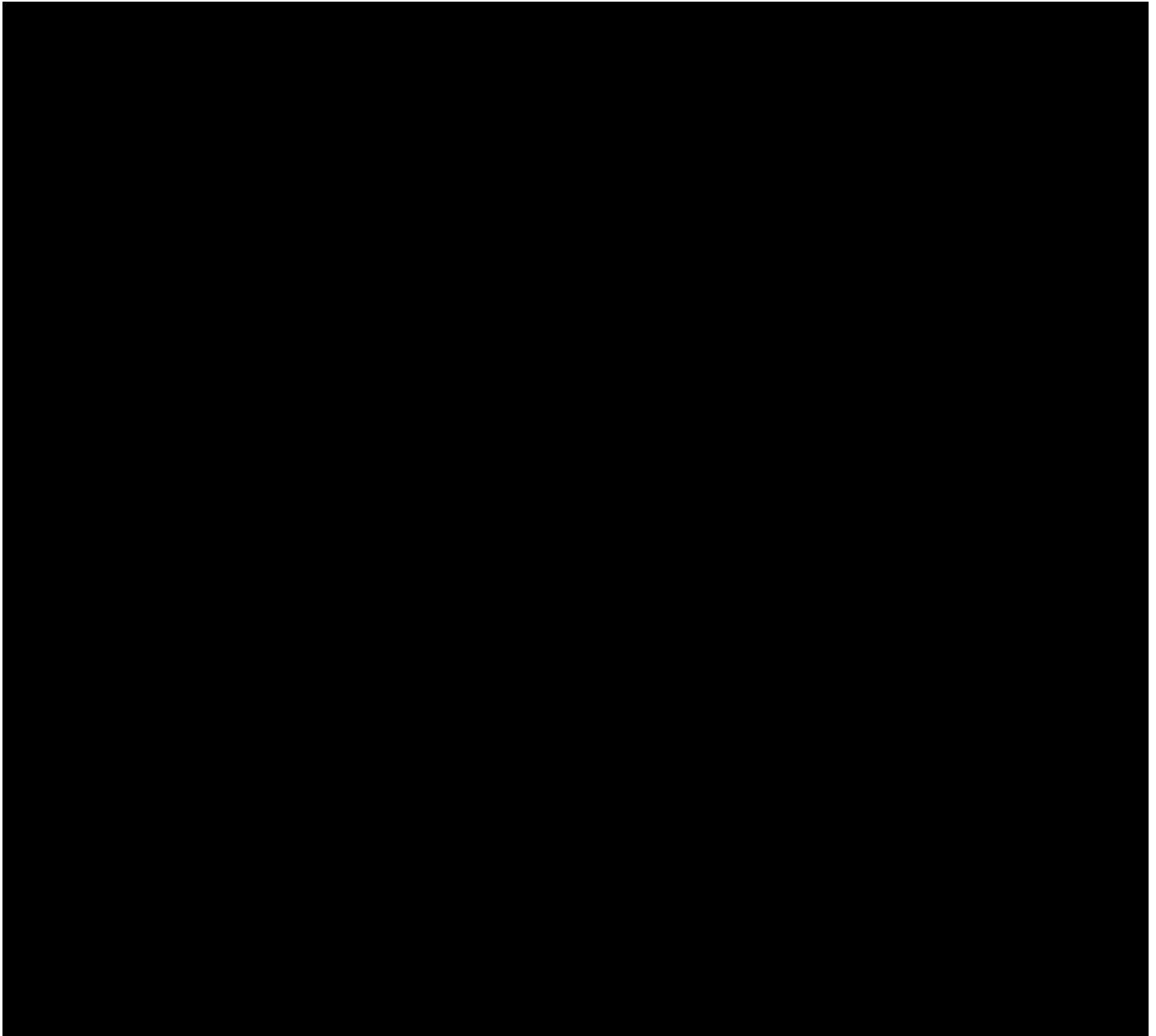
[REDACTED]

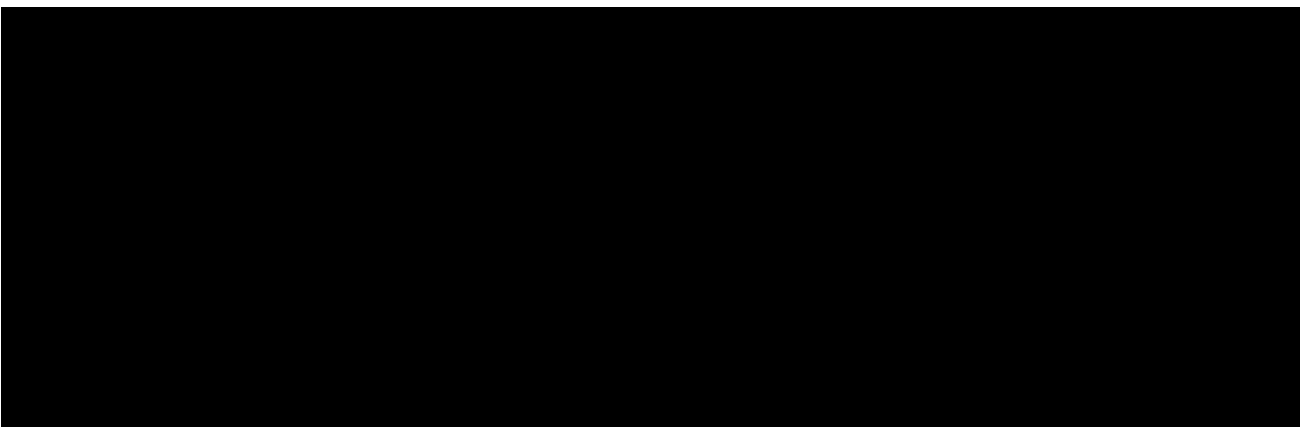
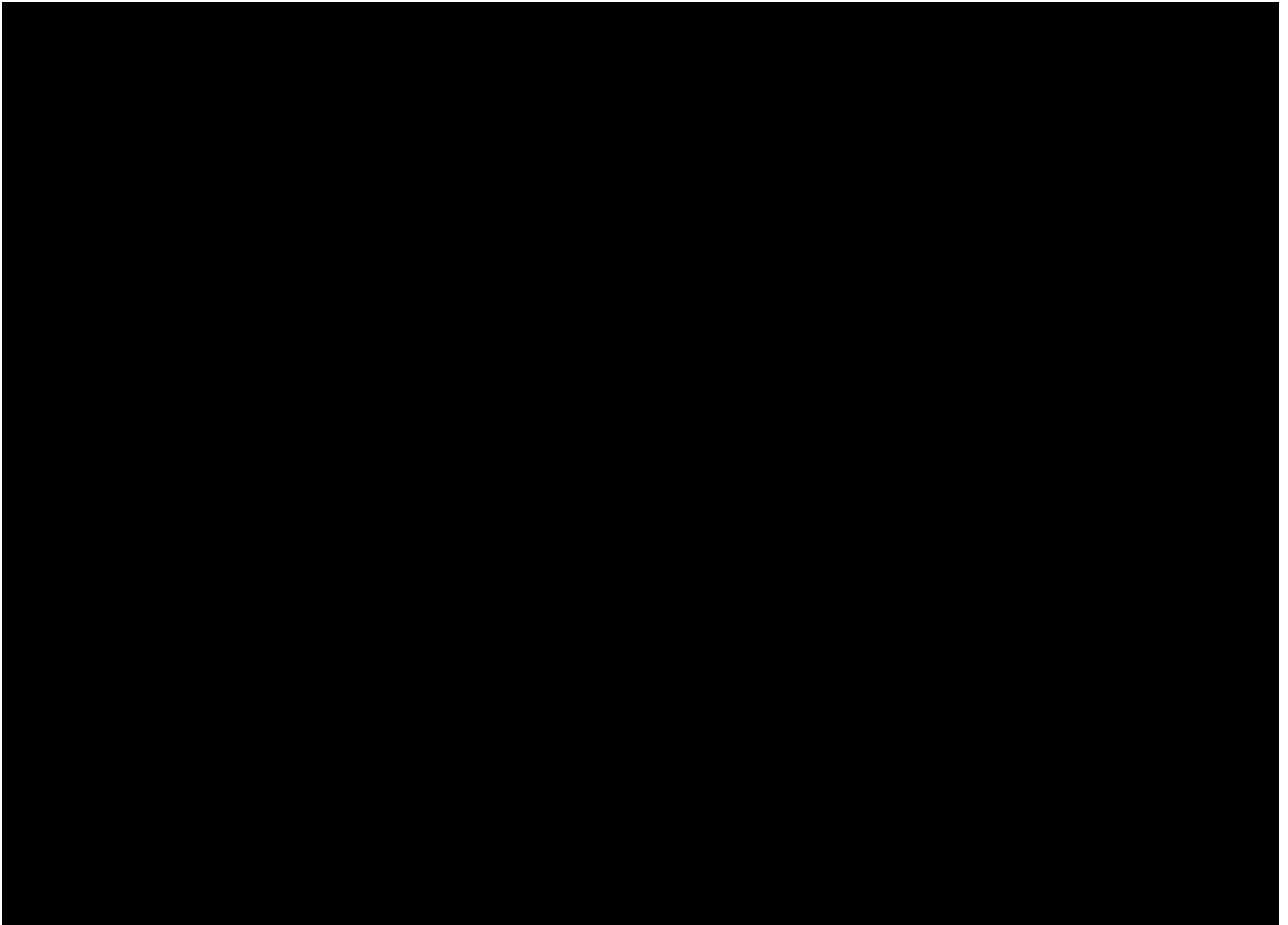




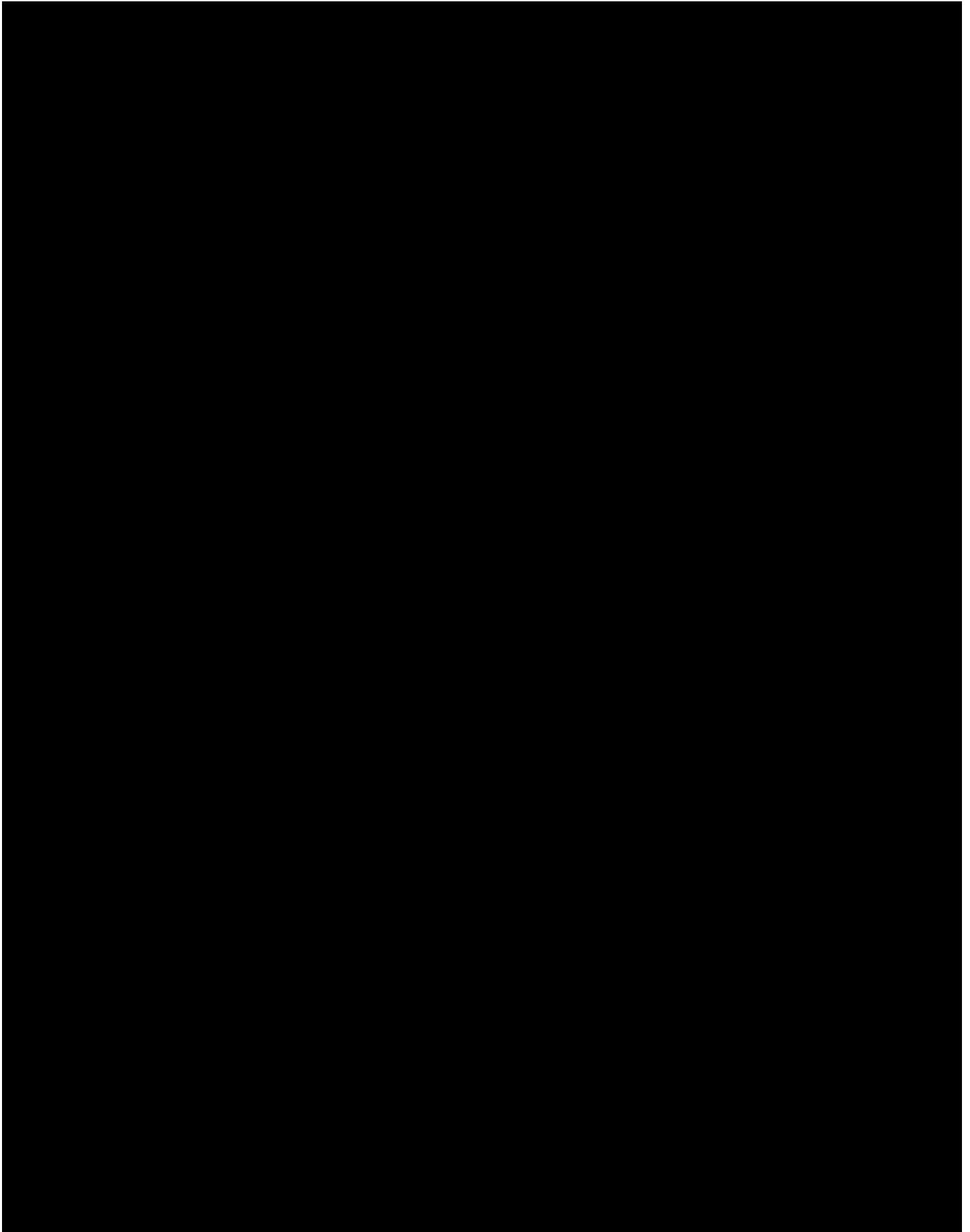


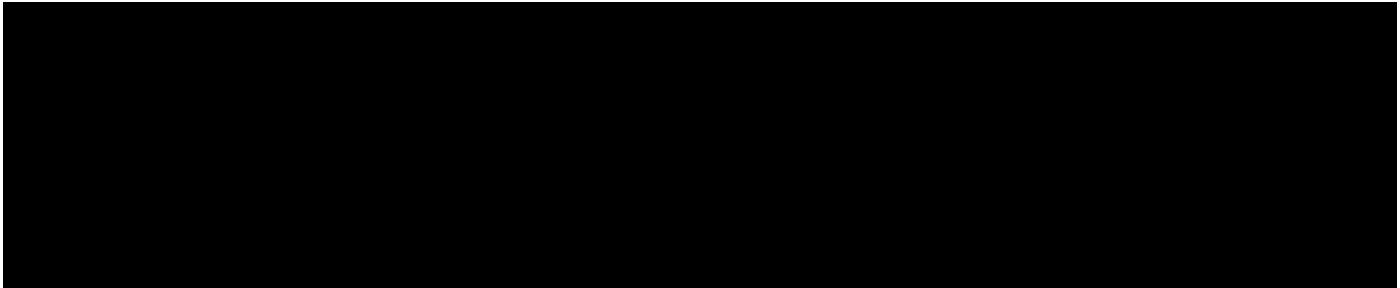
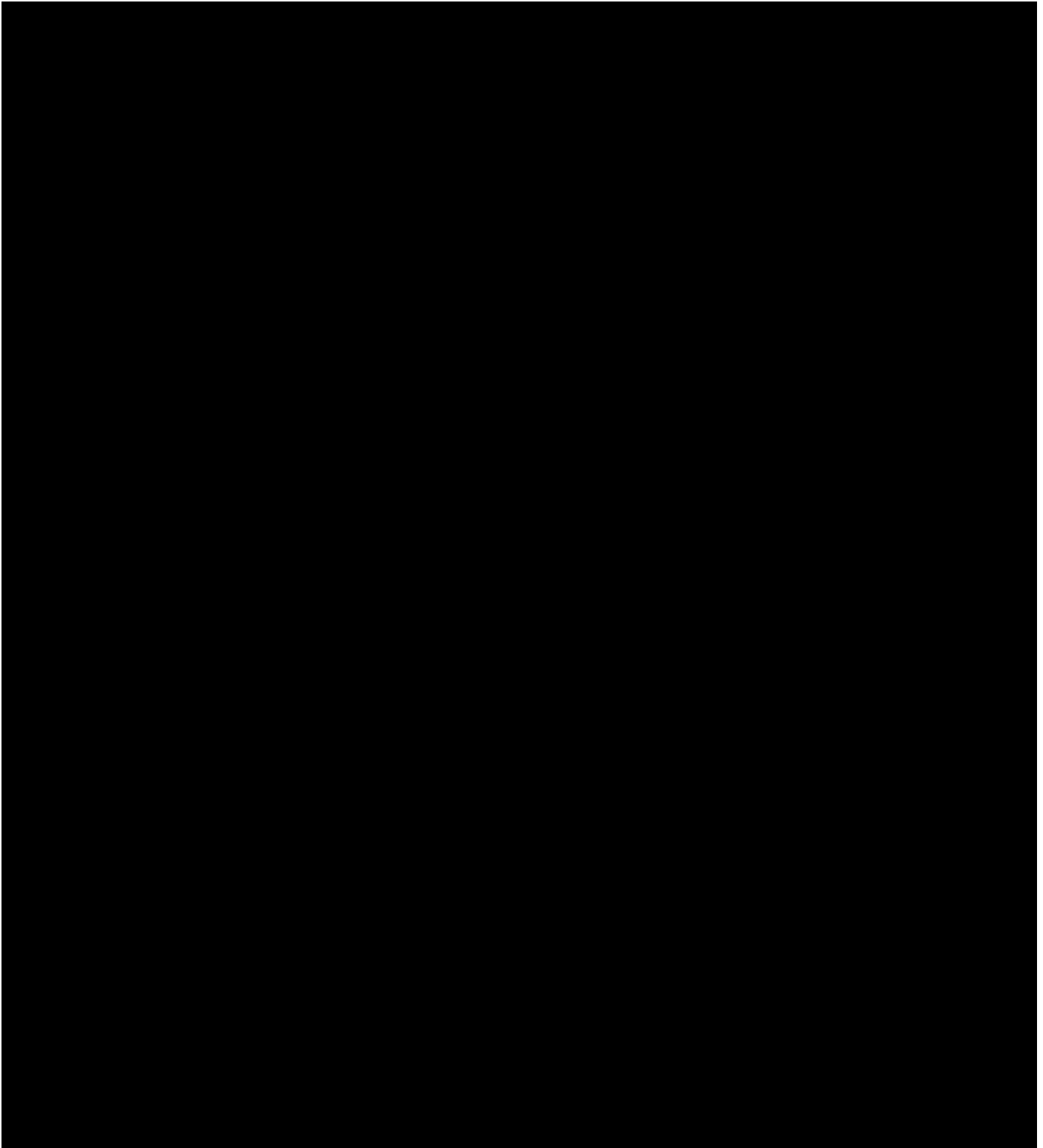








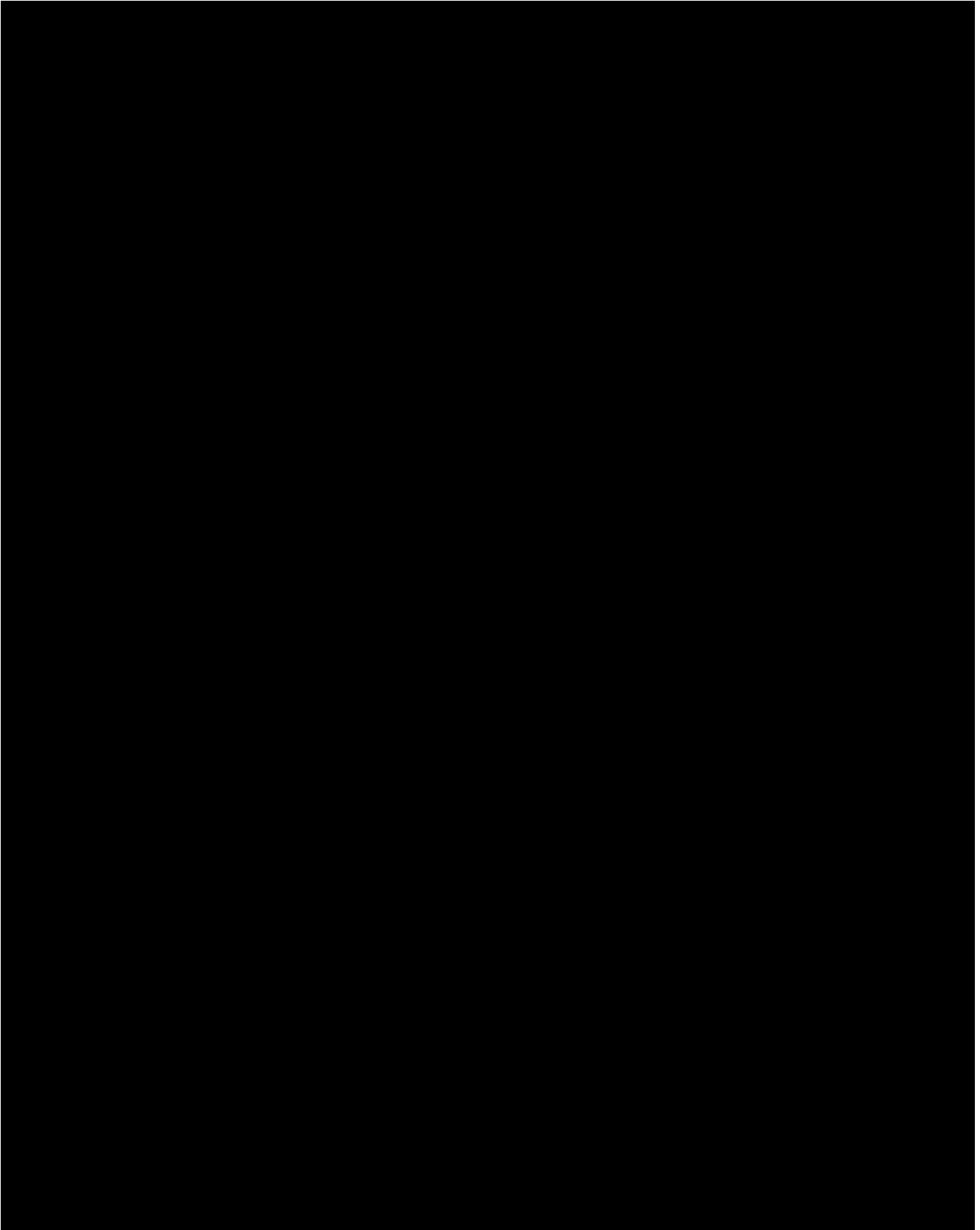


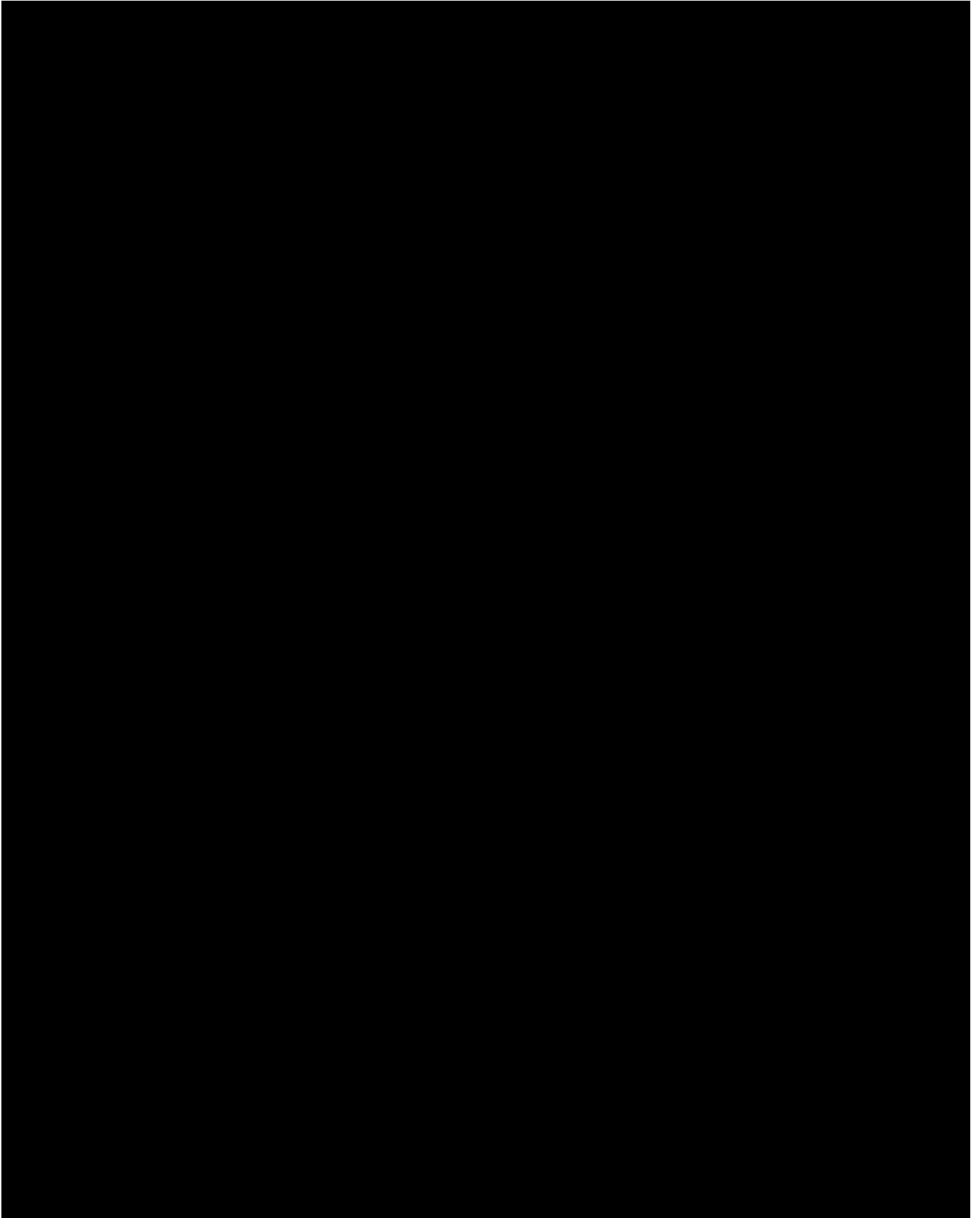


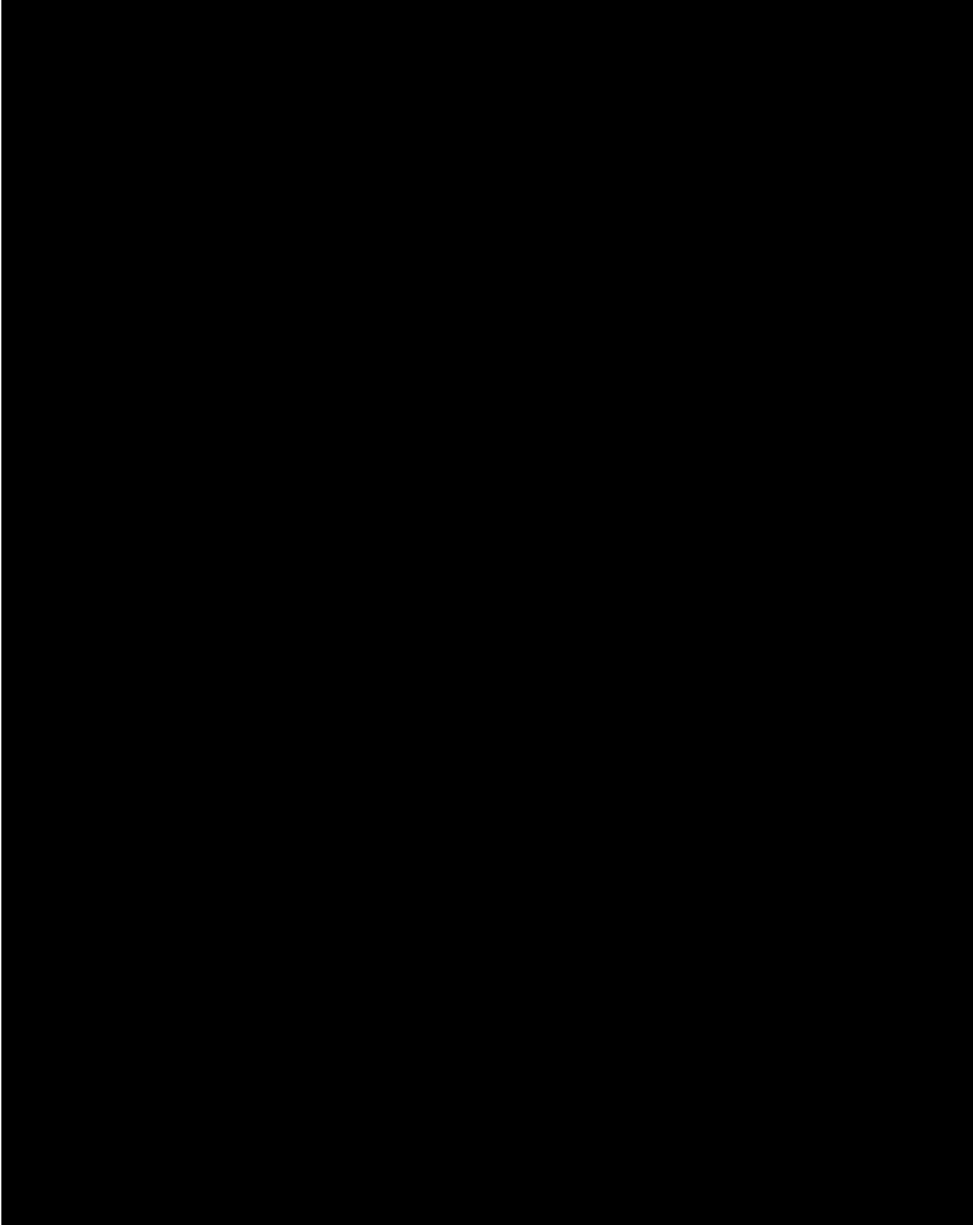


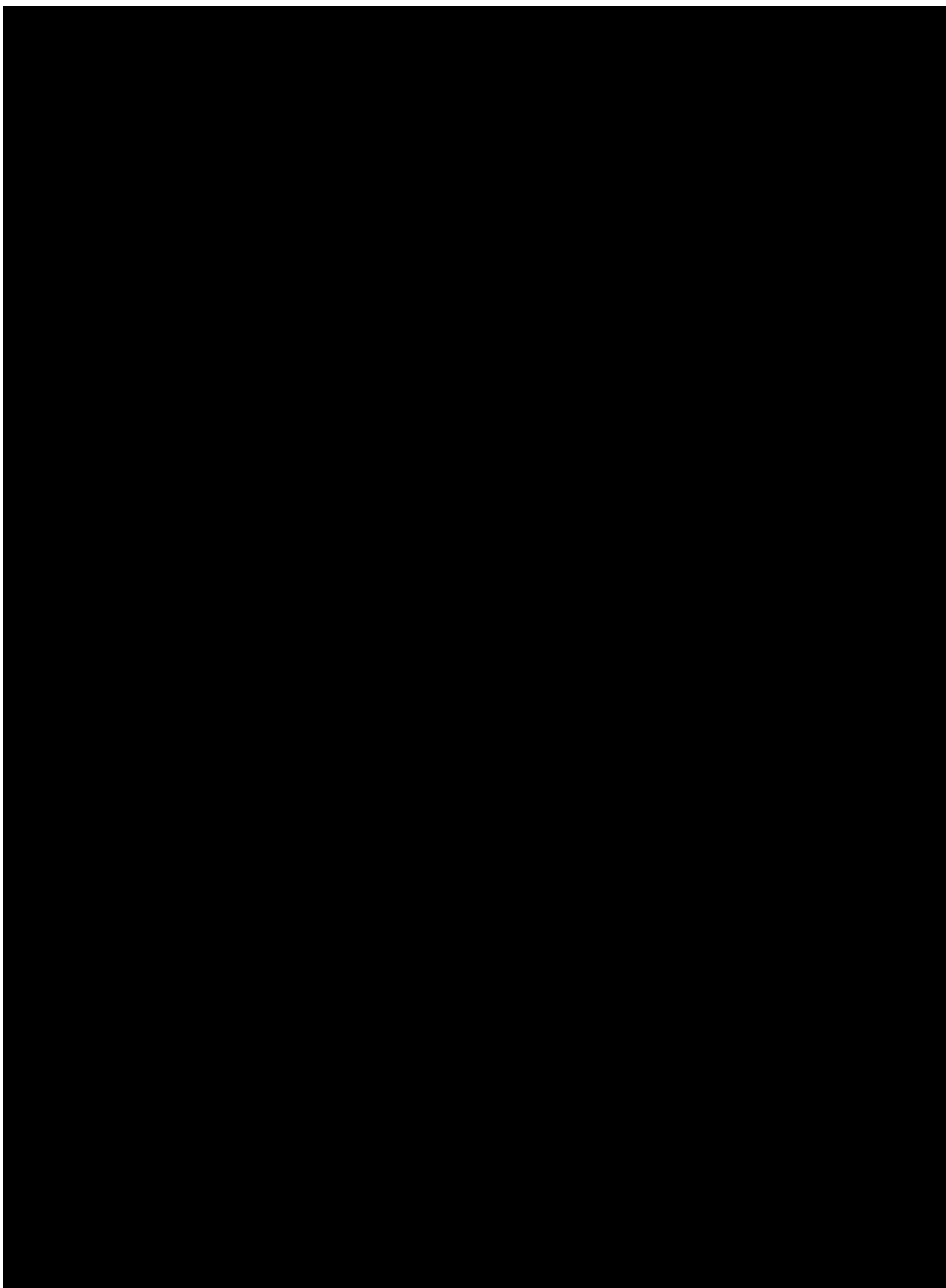




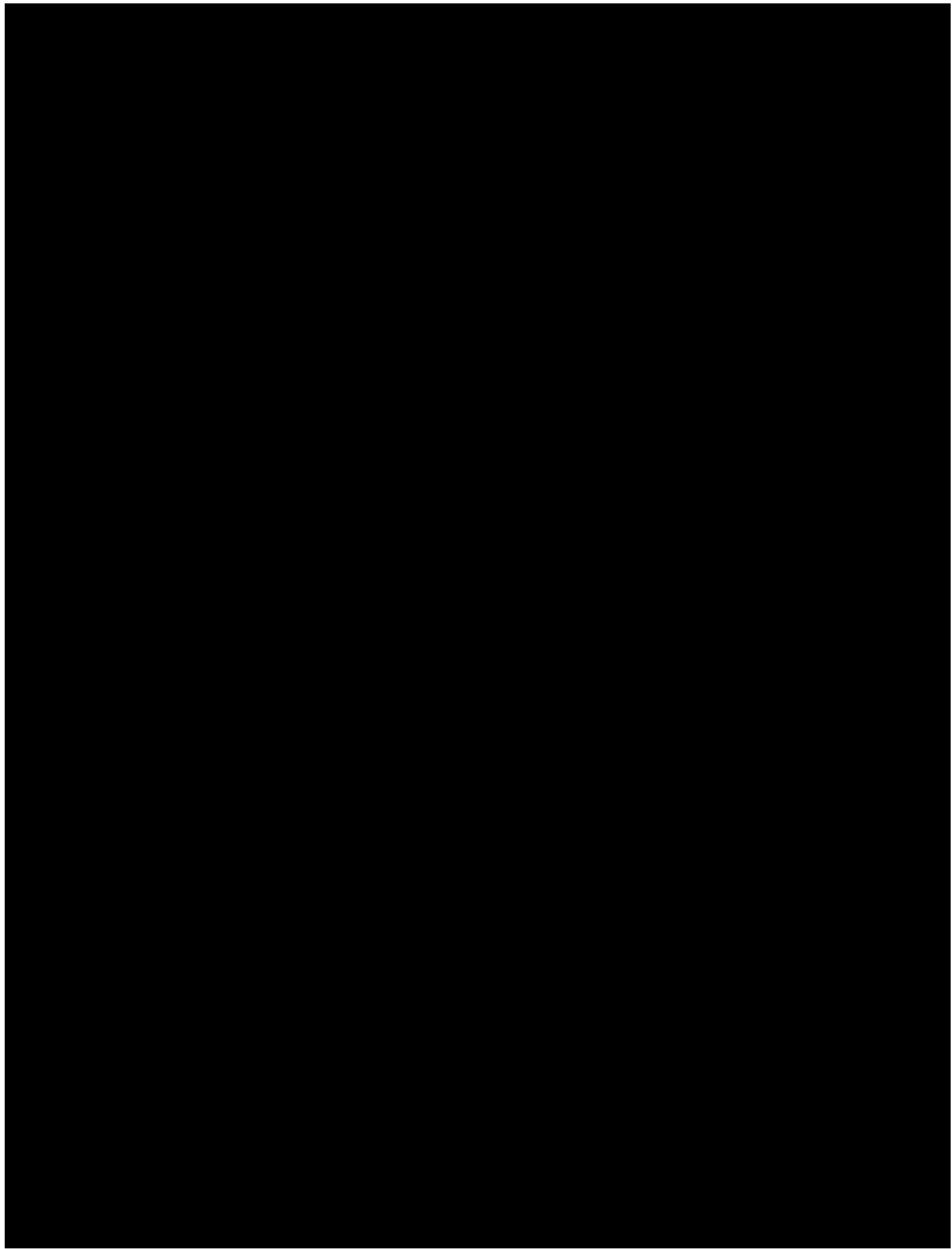


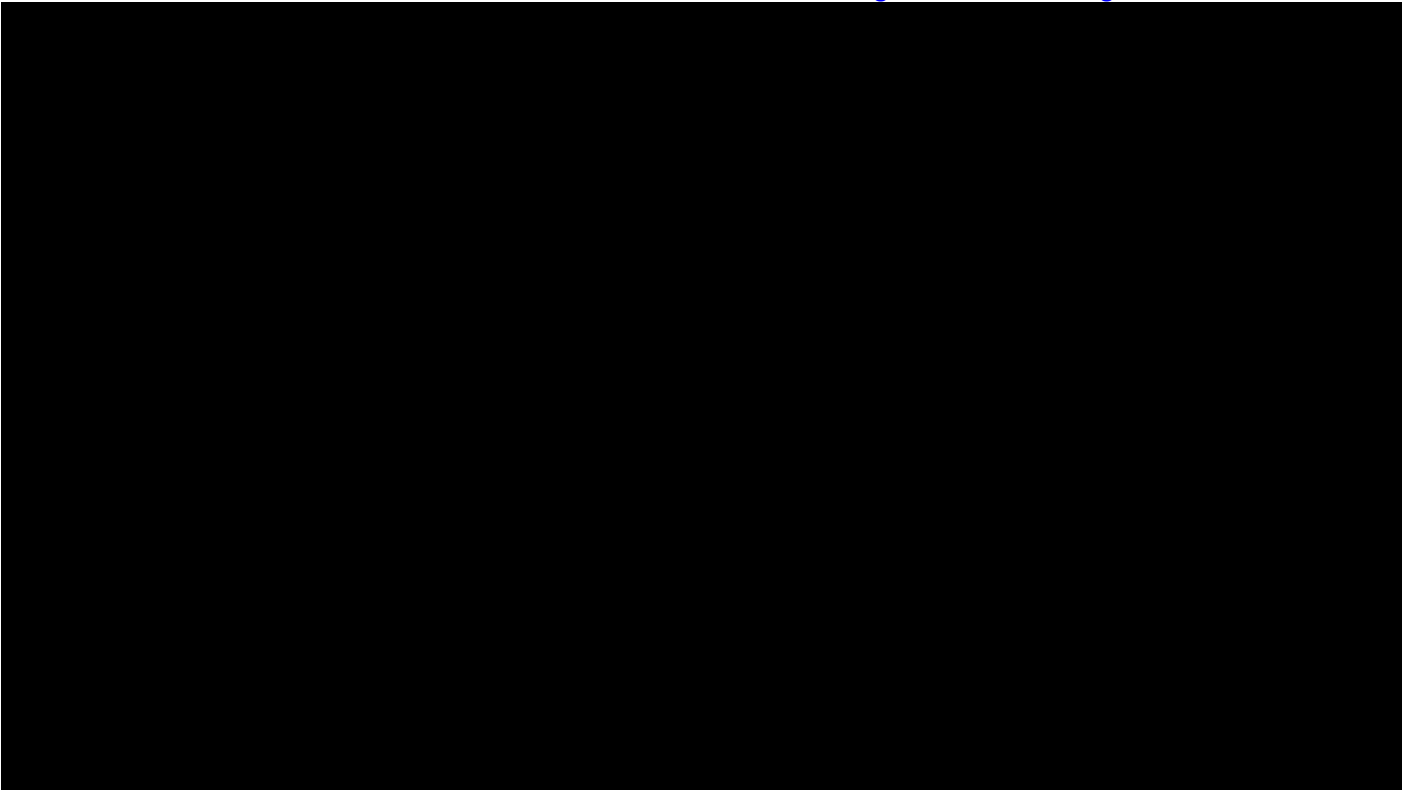


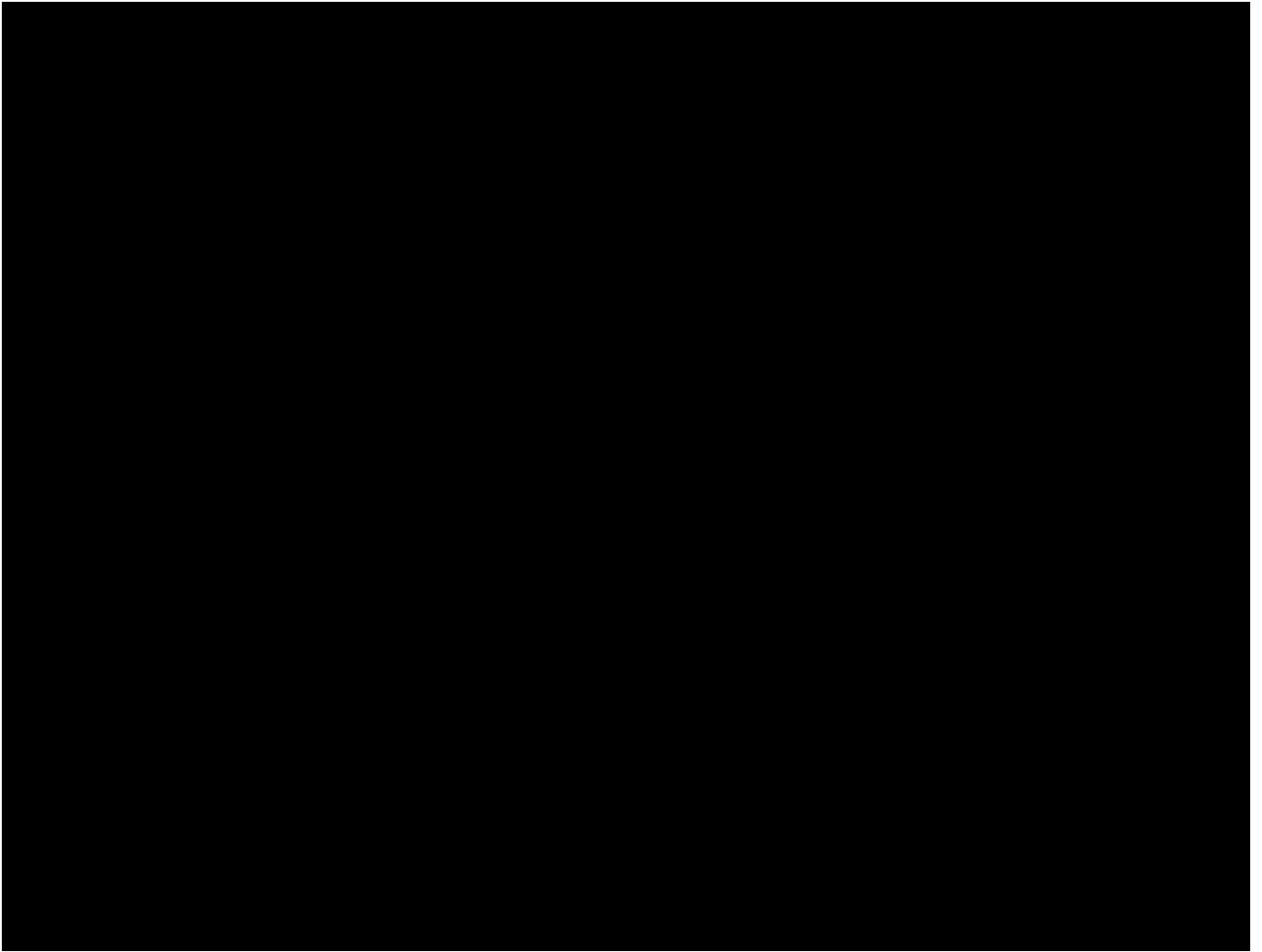




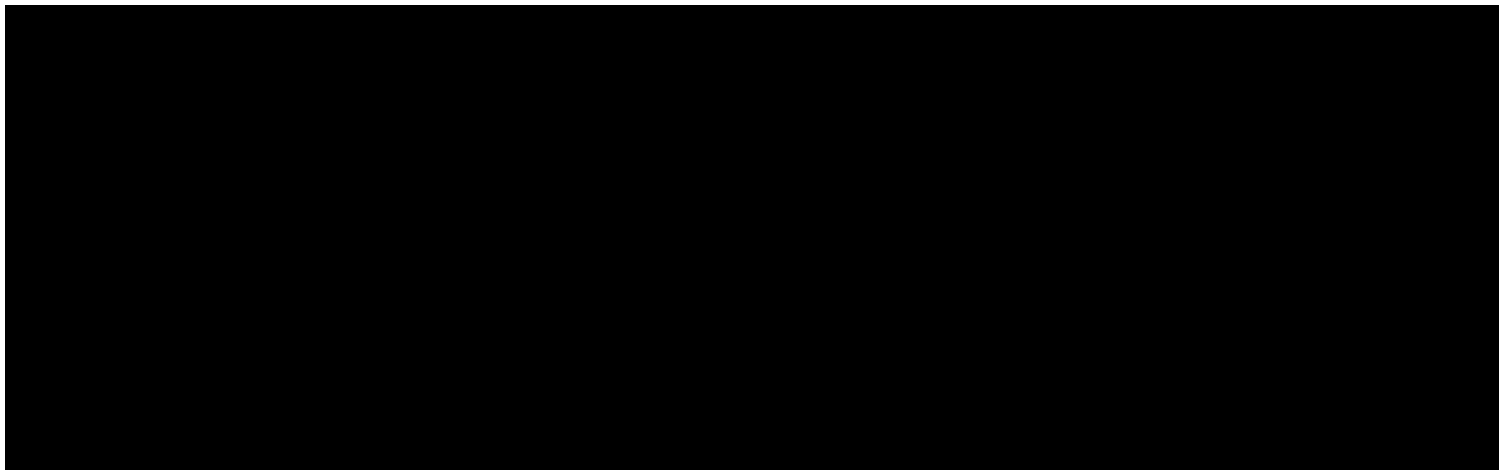
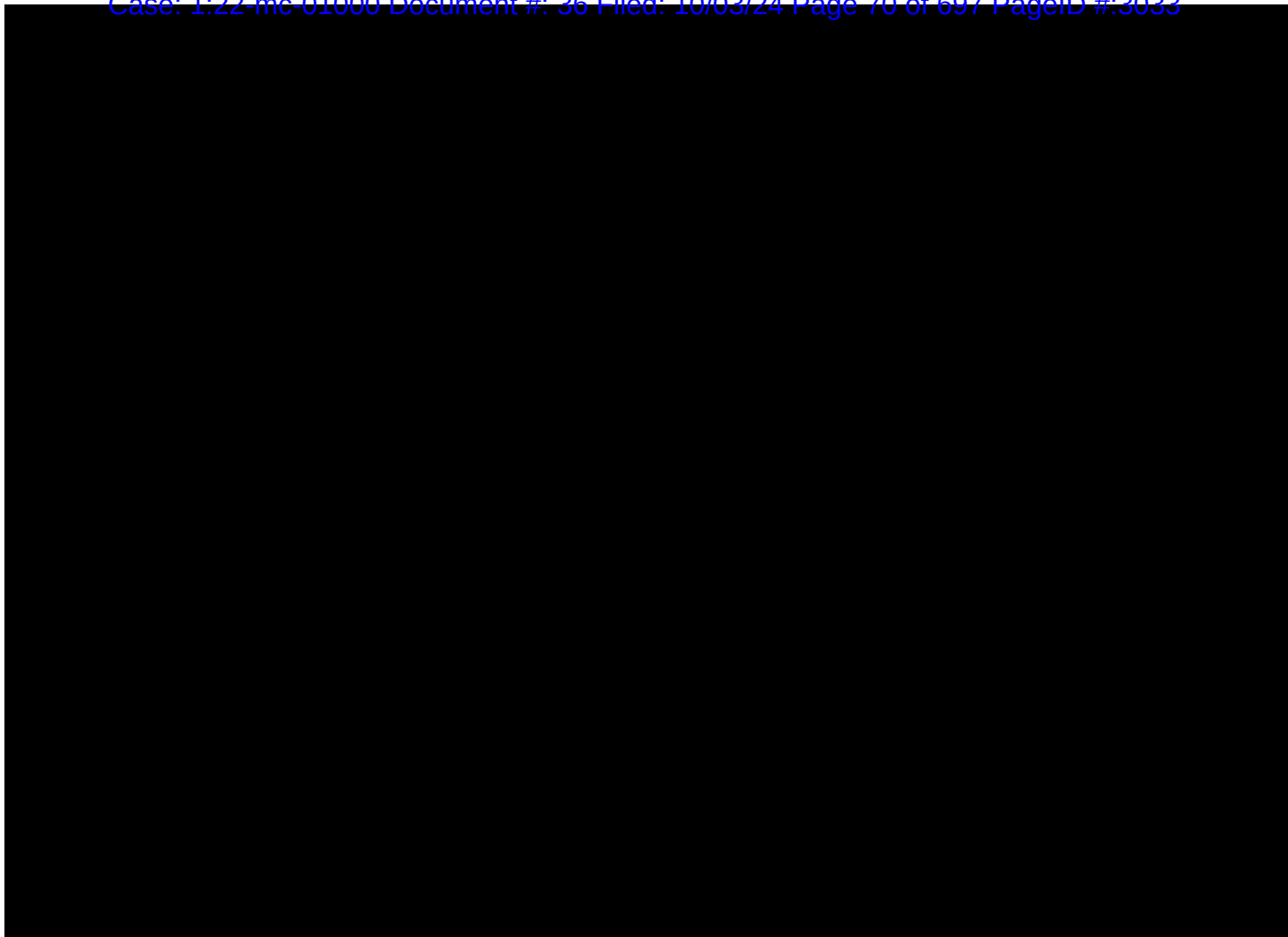


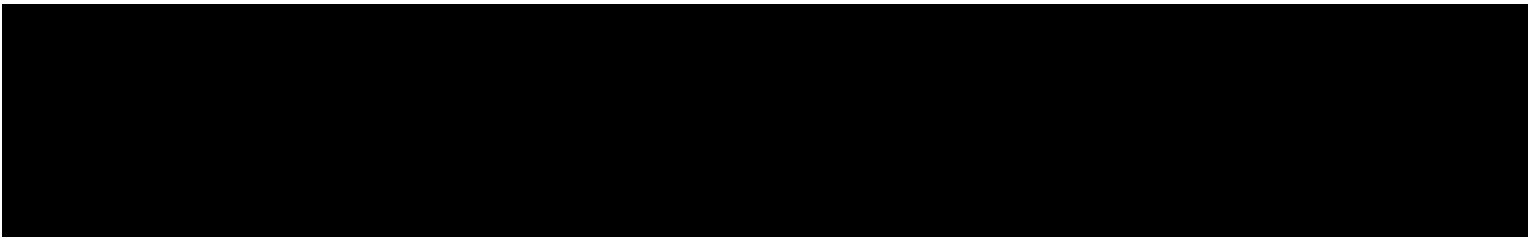
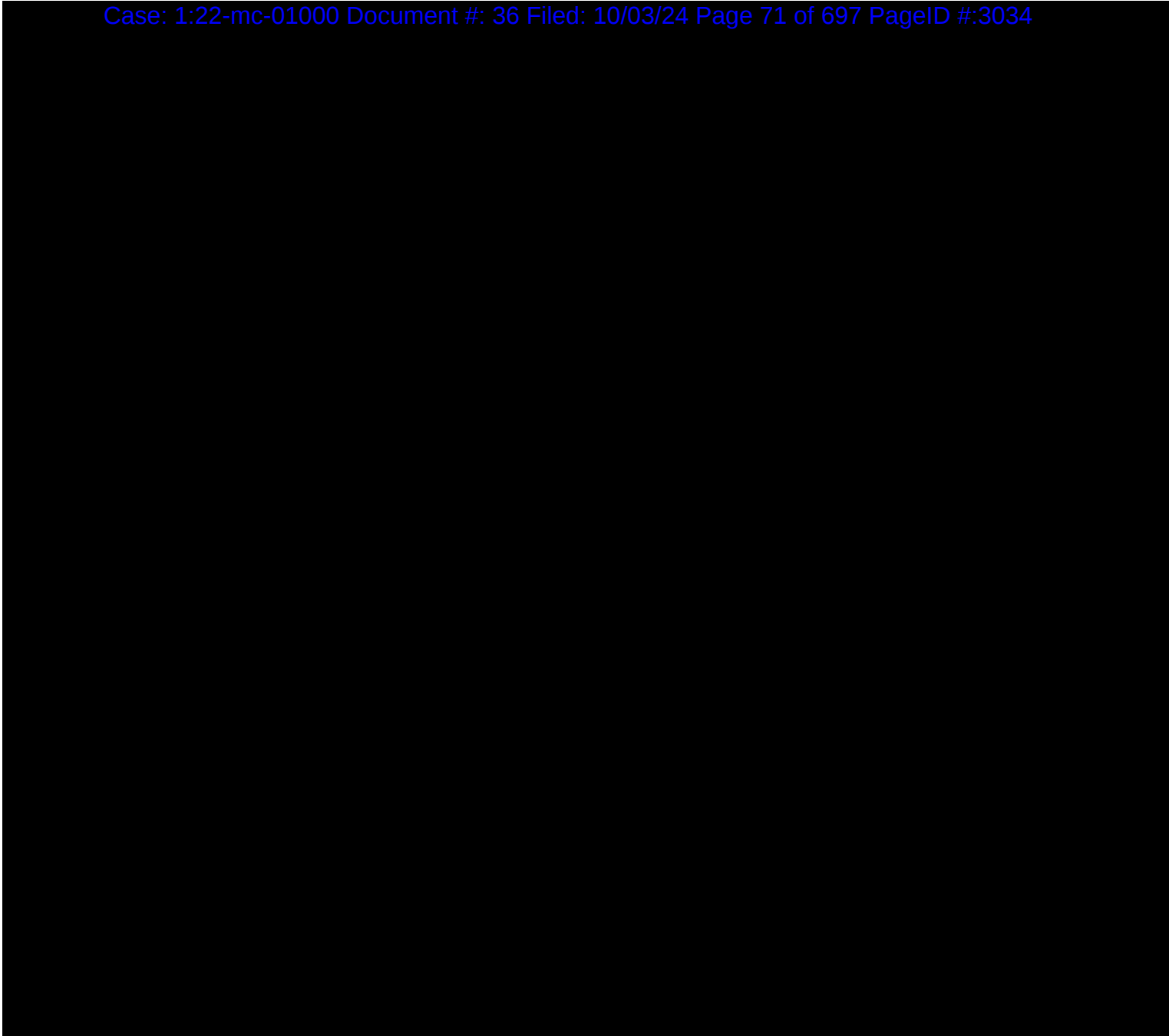


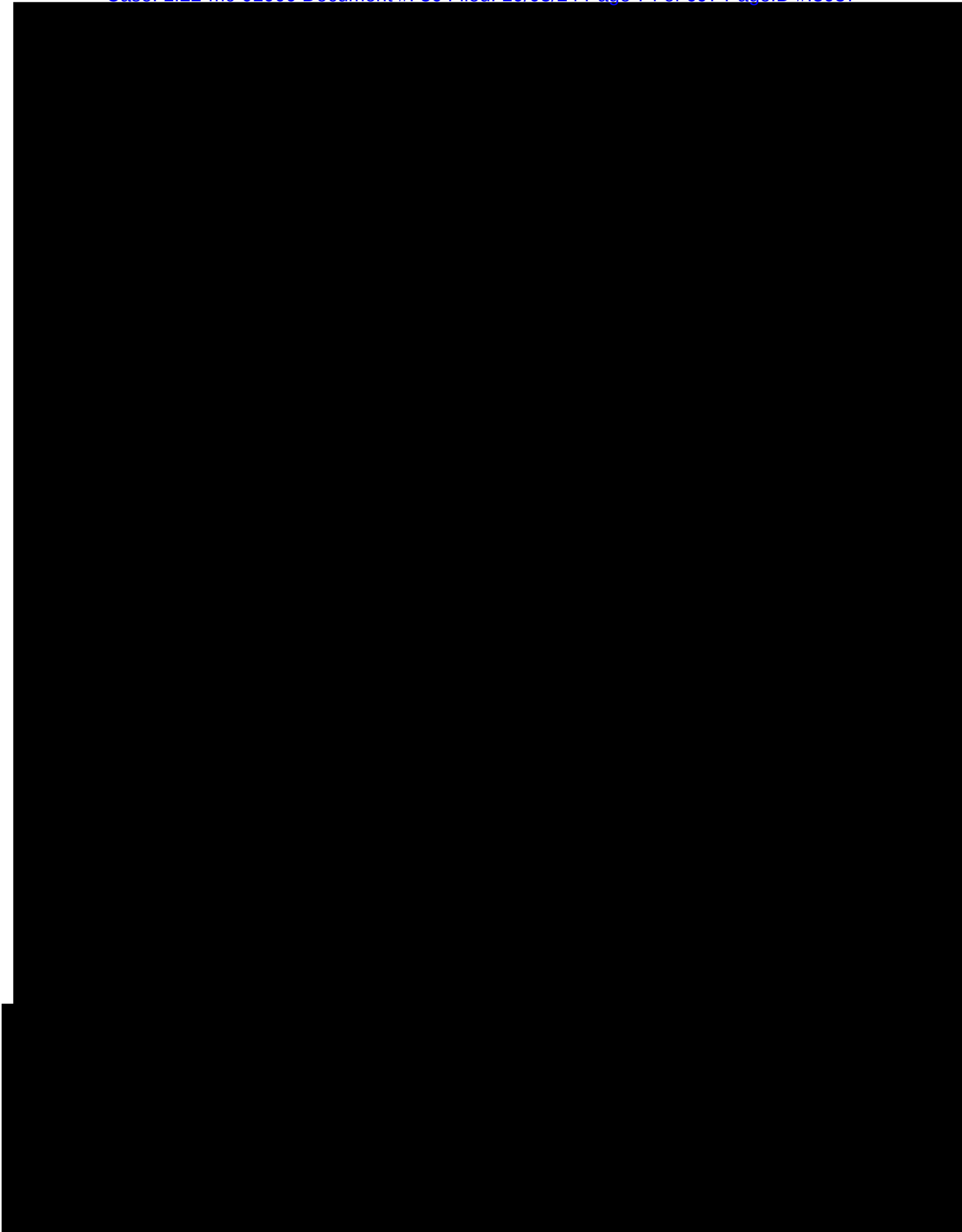


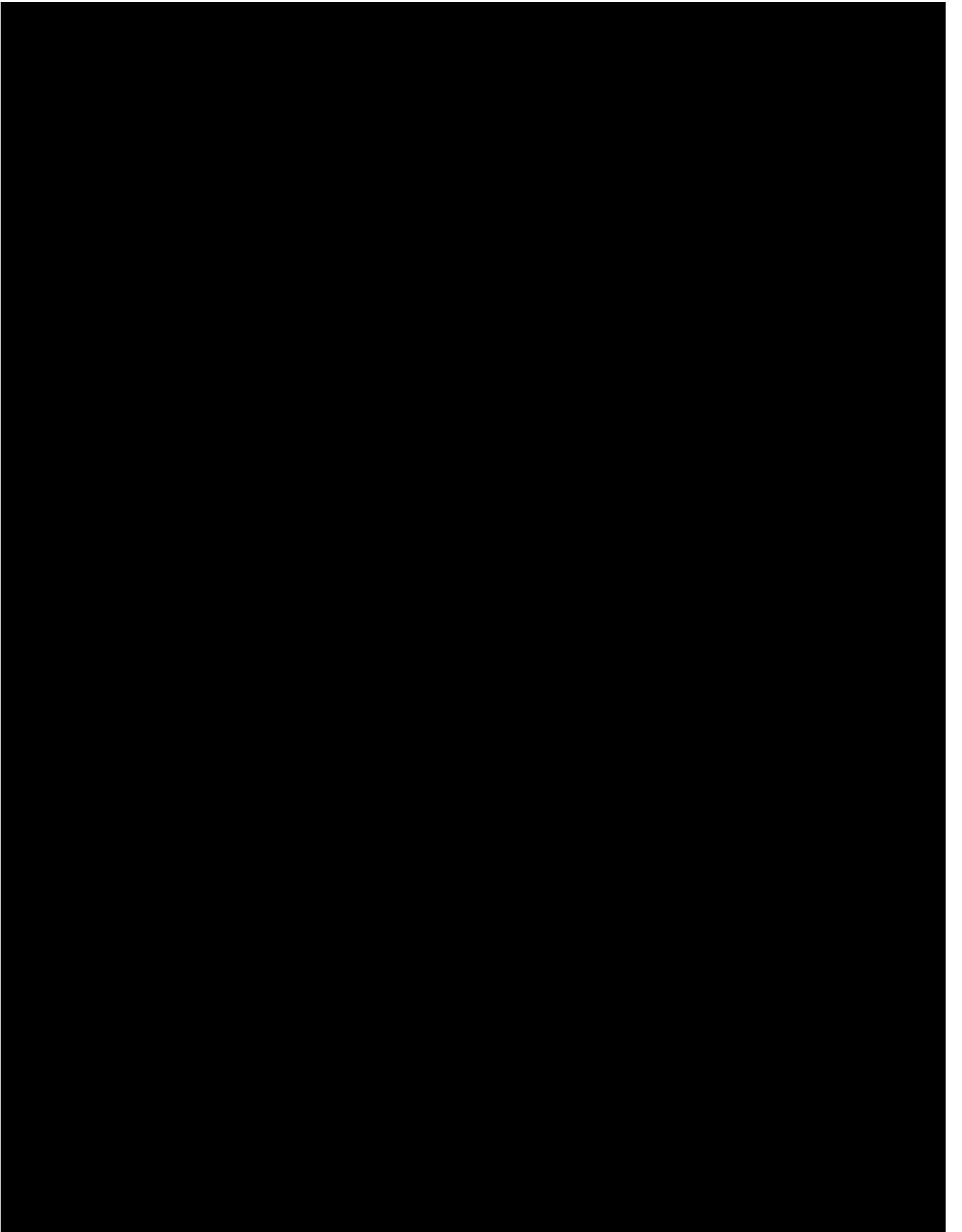


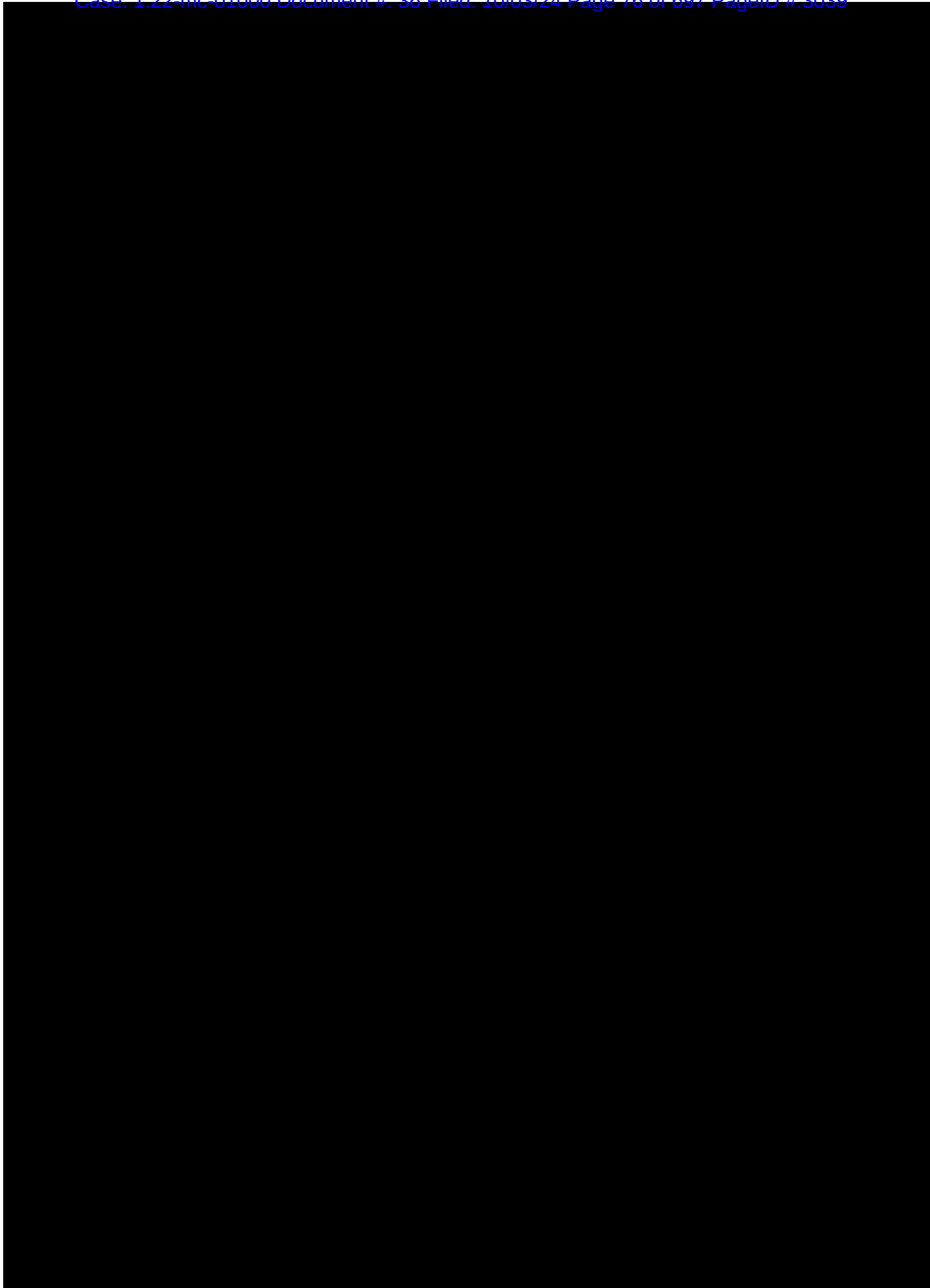


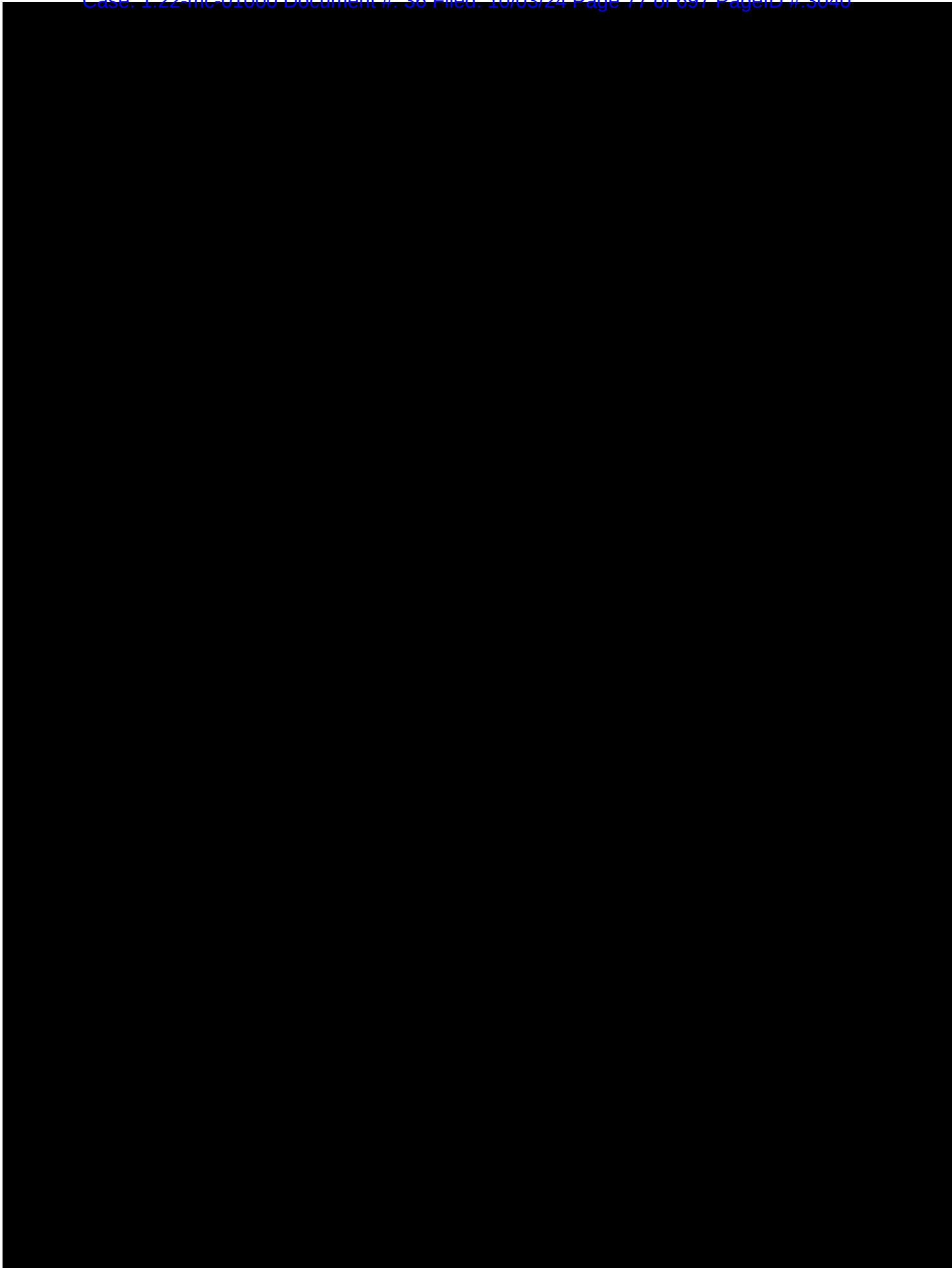


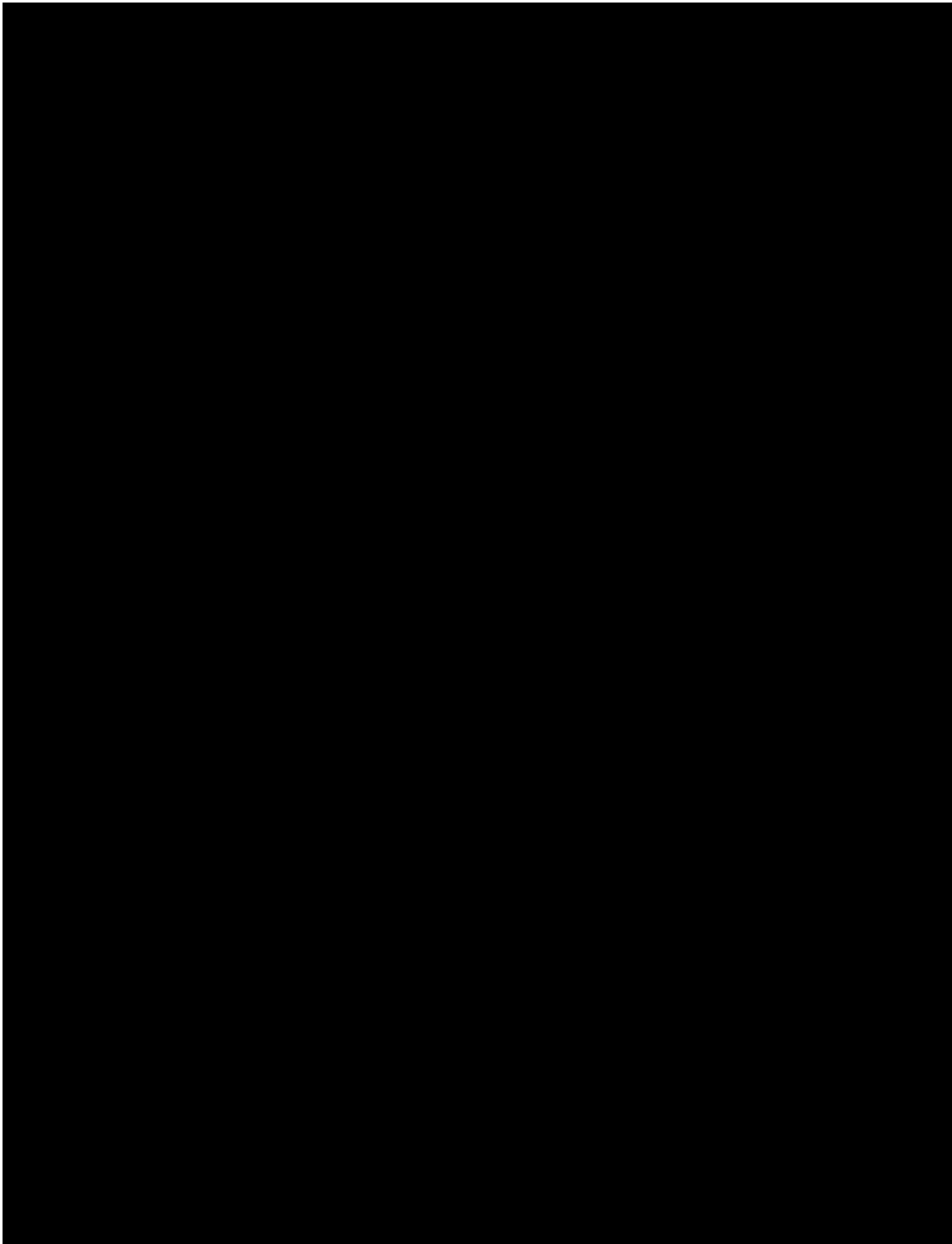


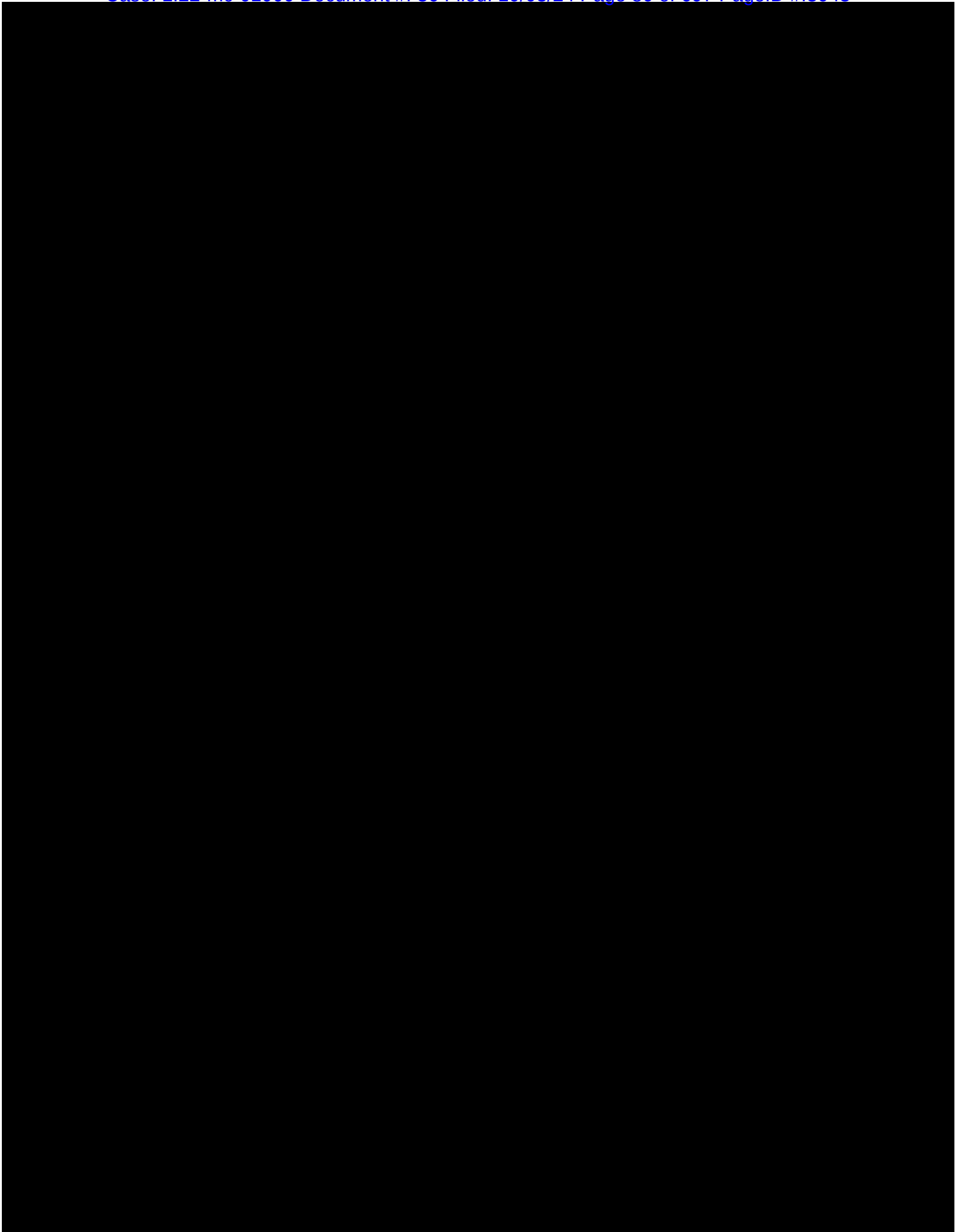




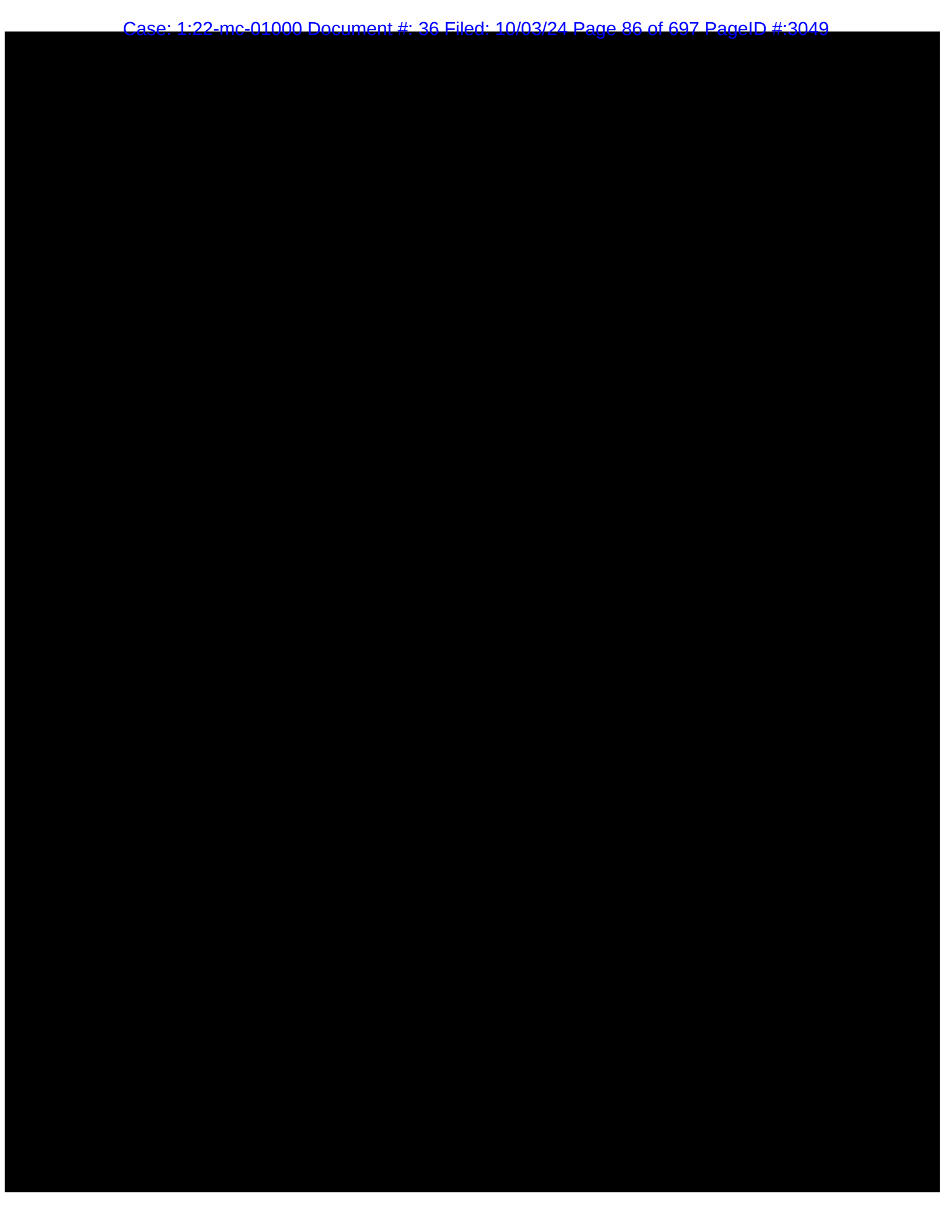


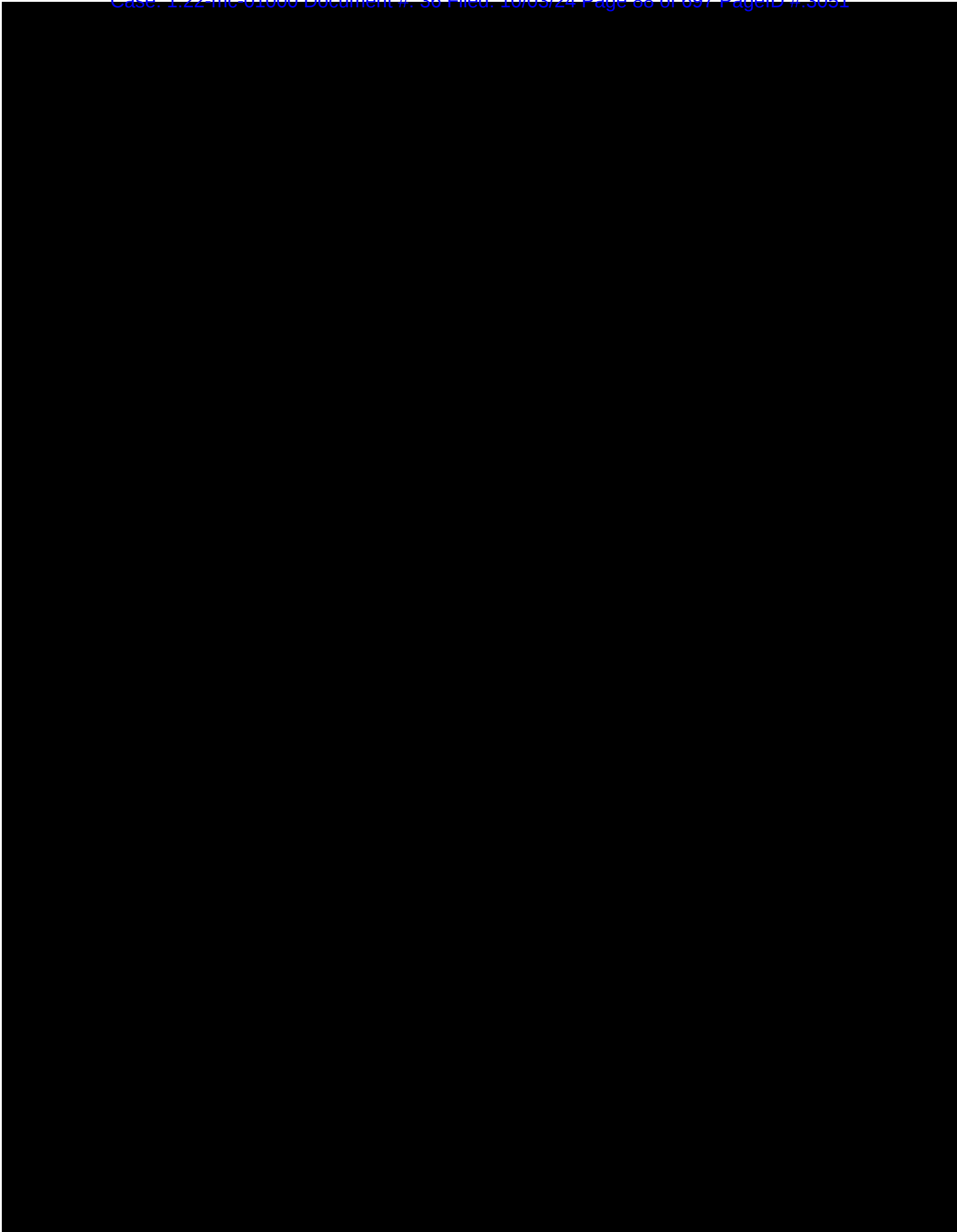


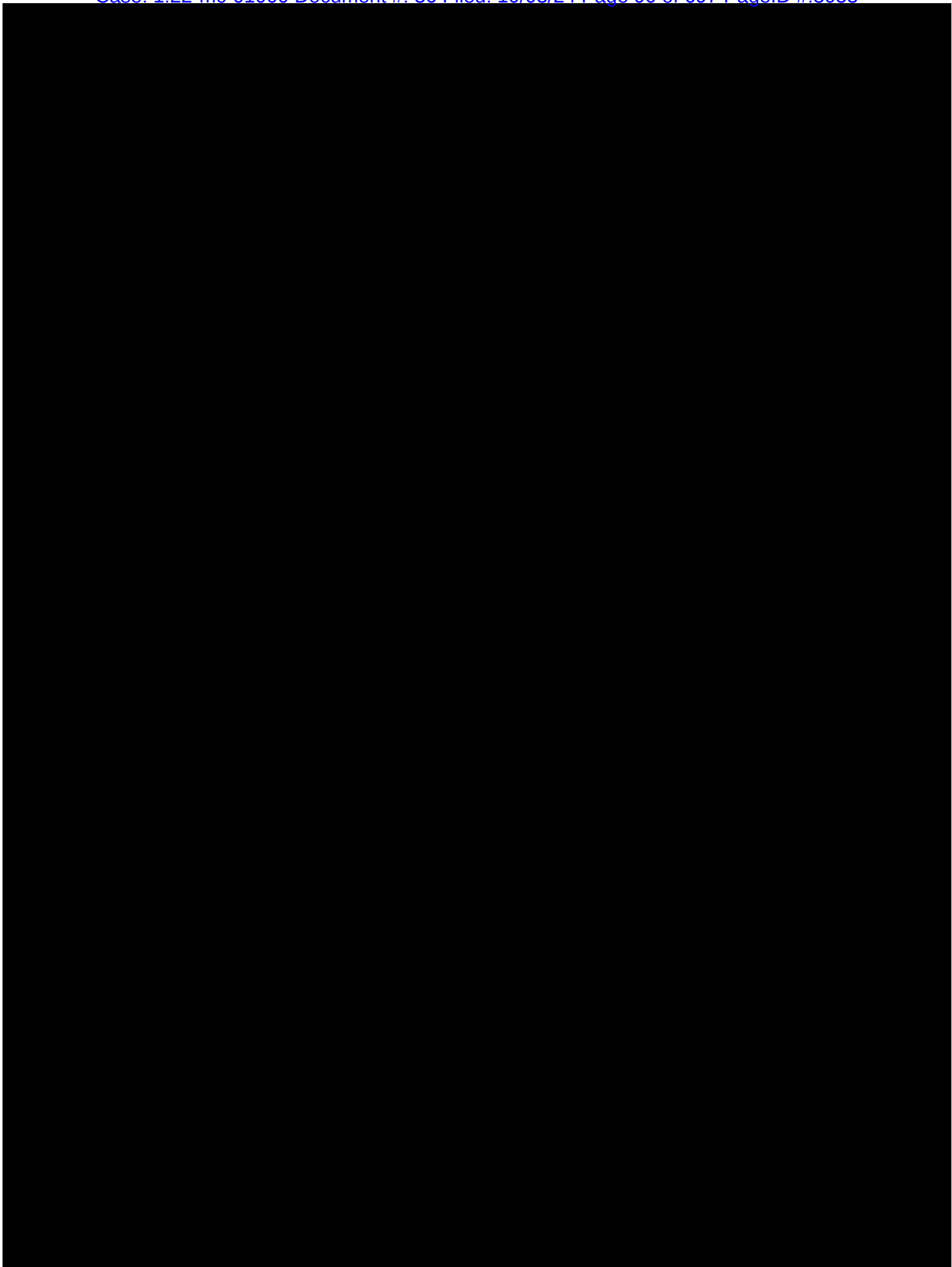


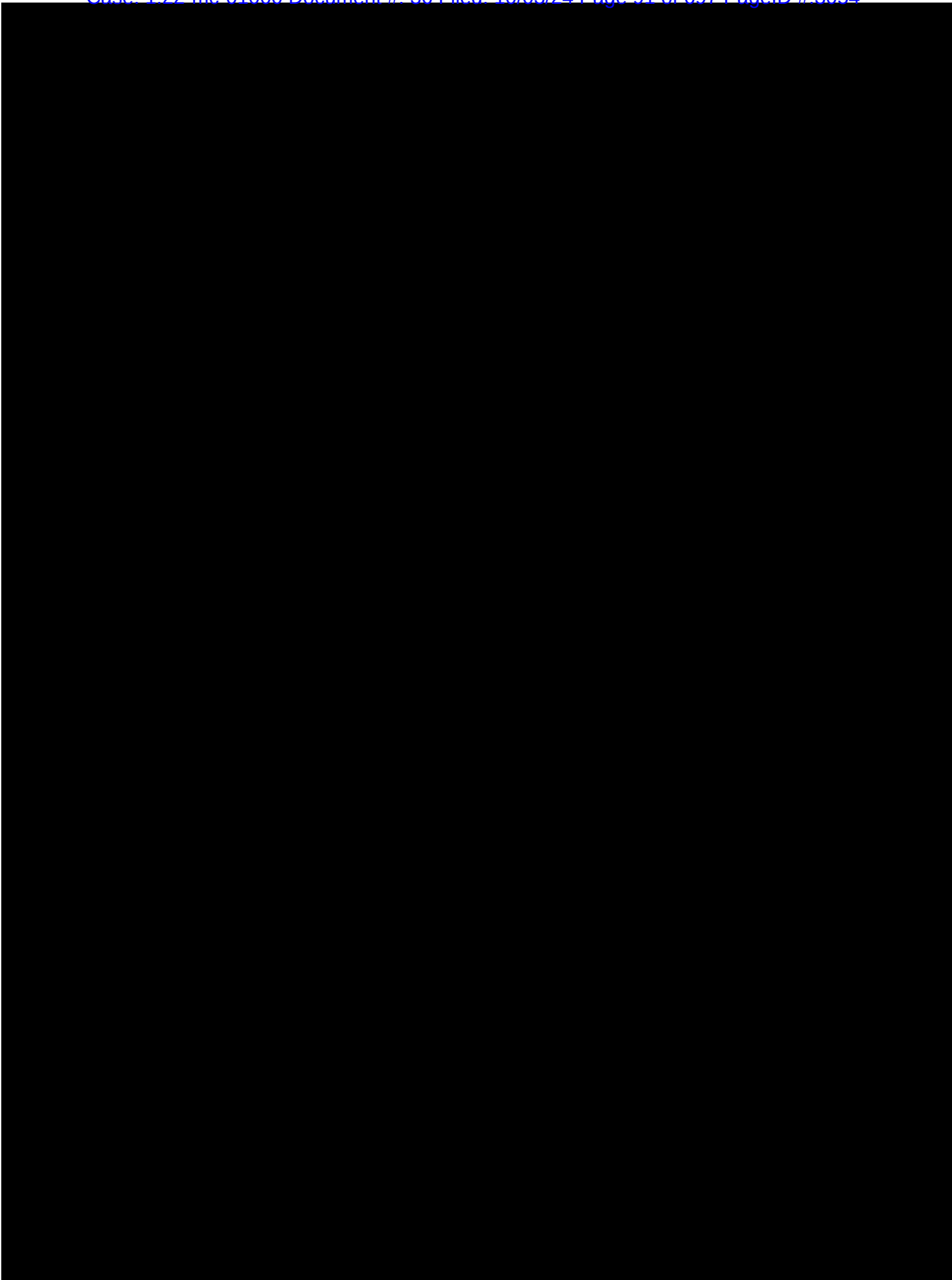


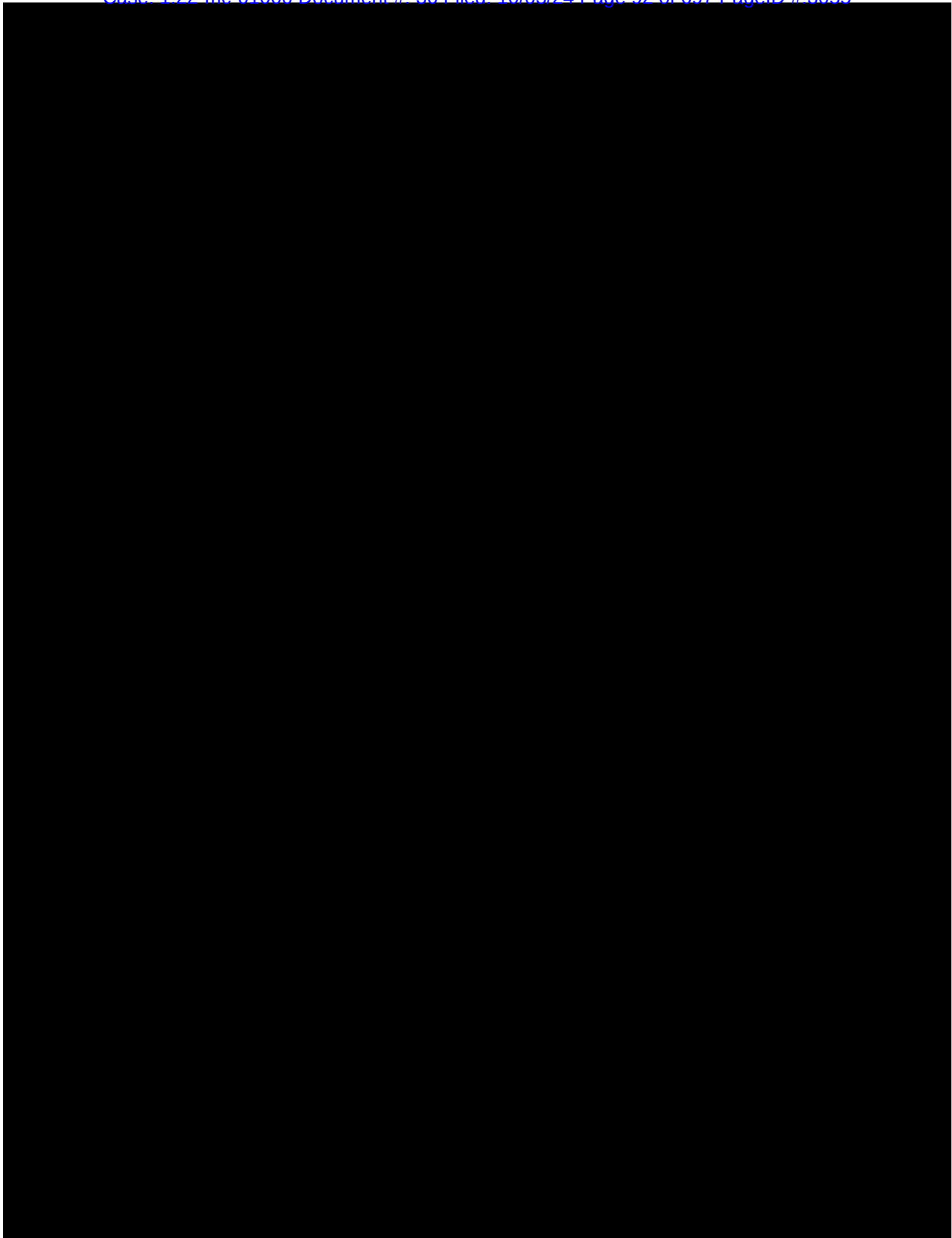
[illegible]

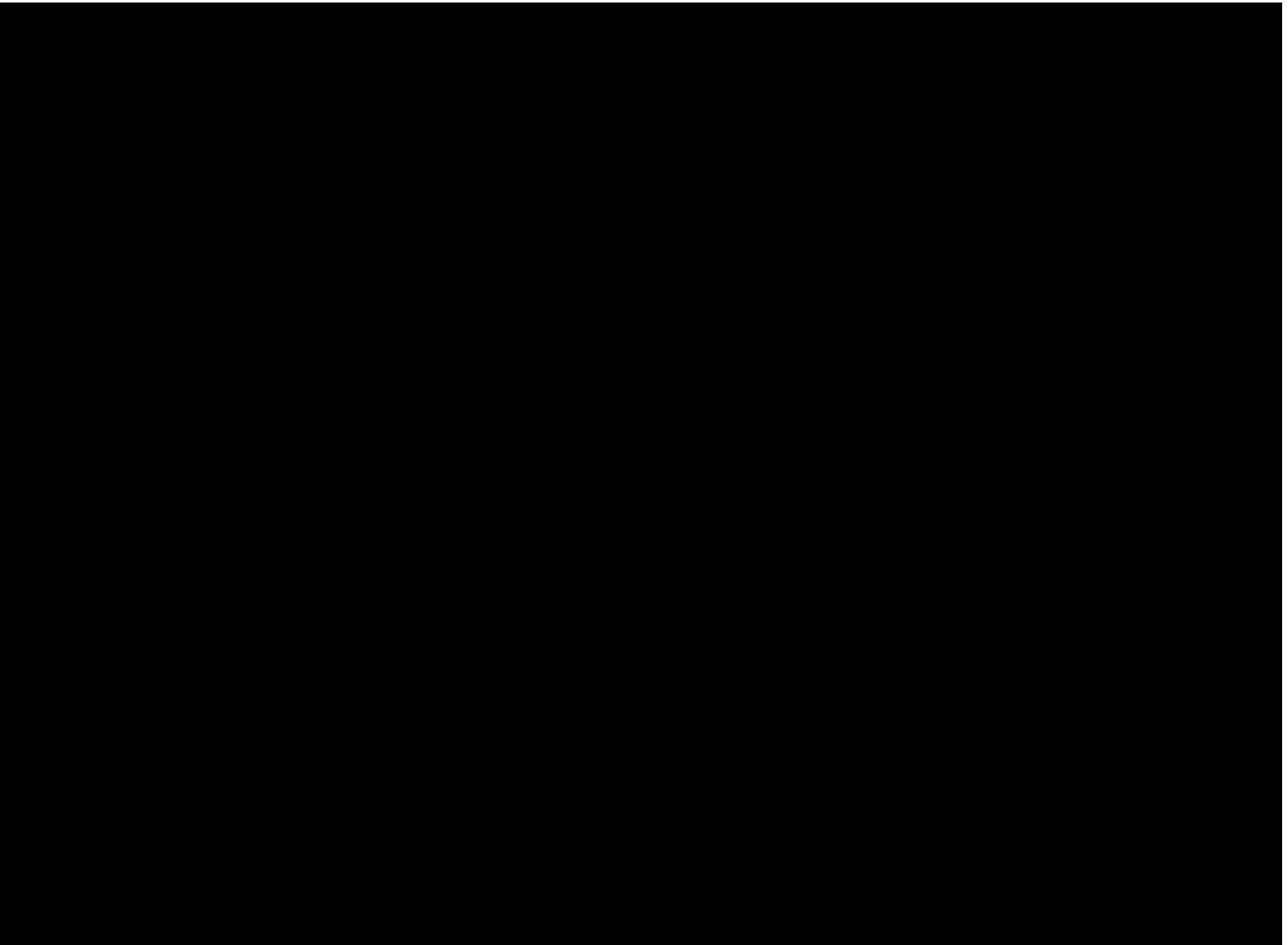


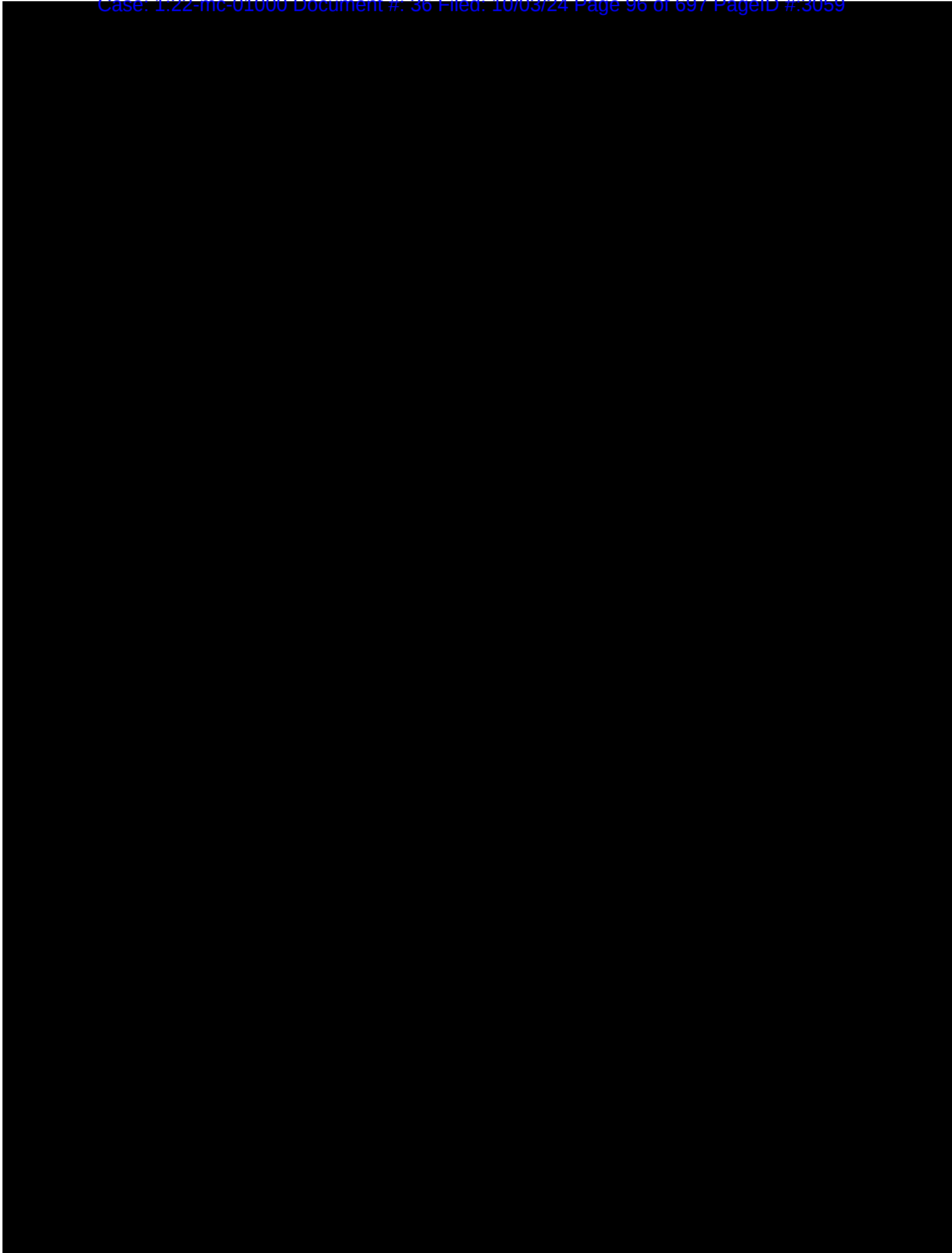


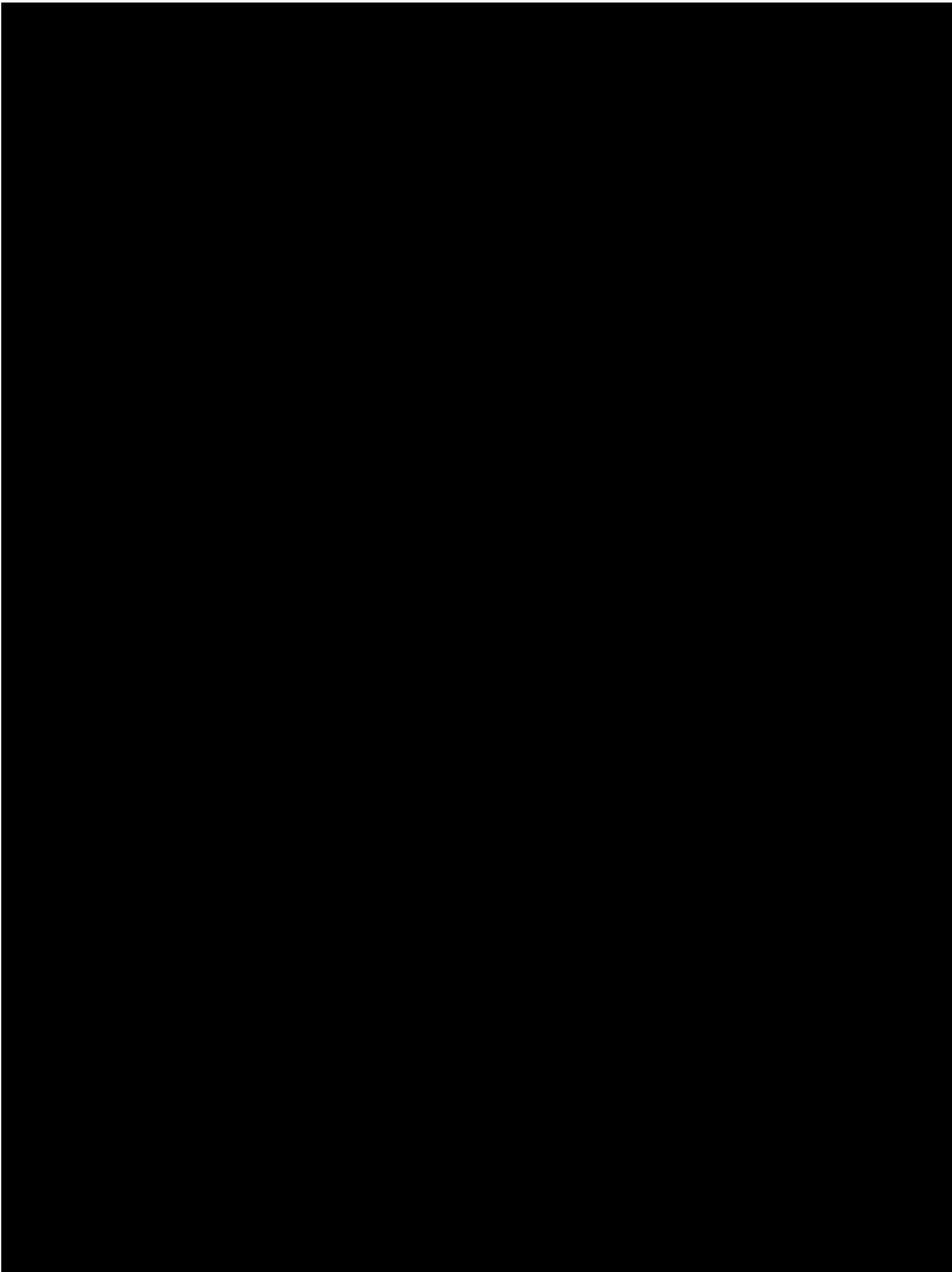


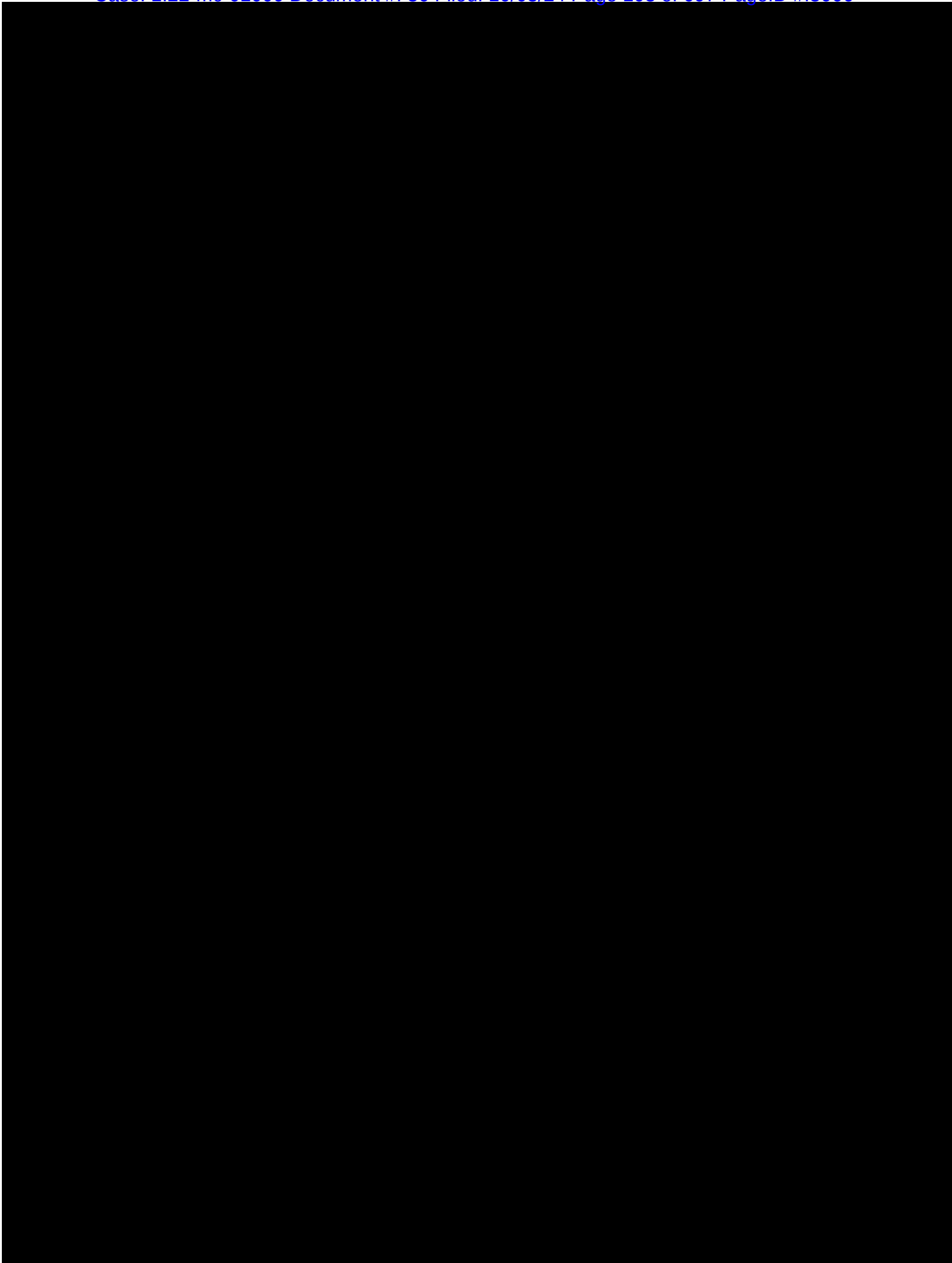


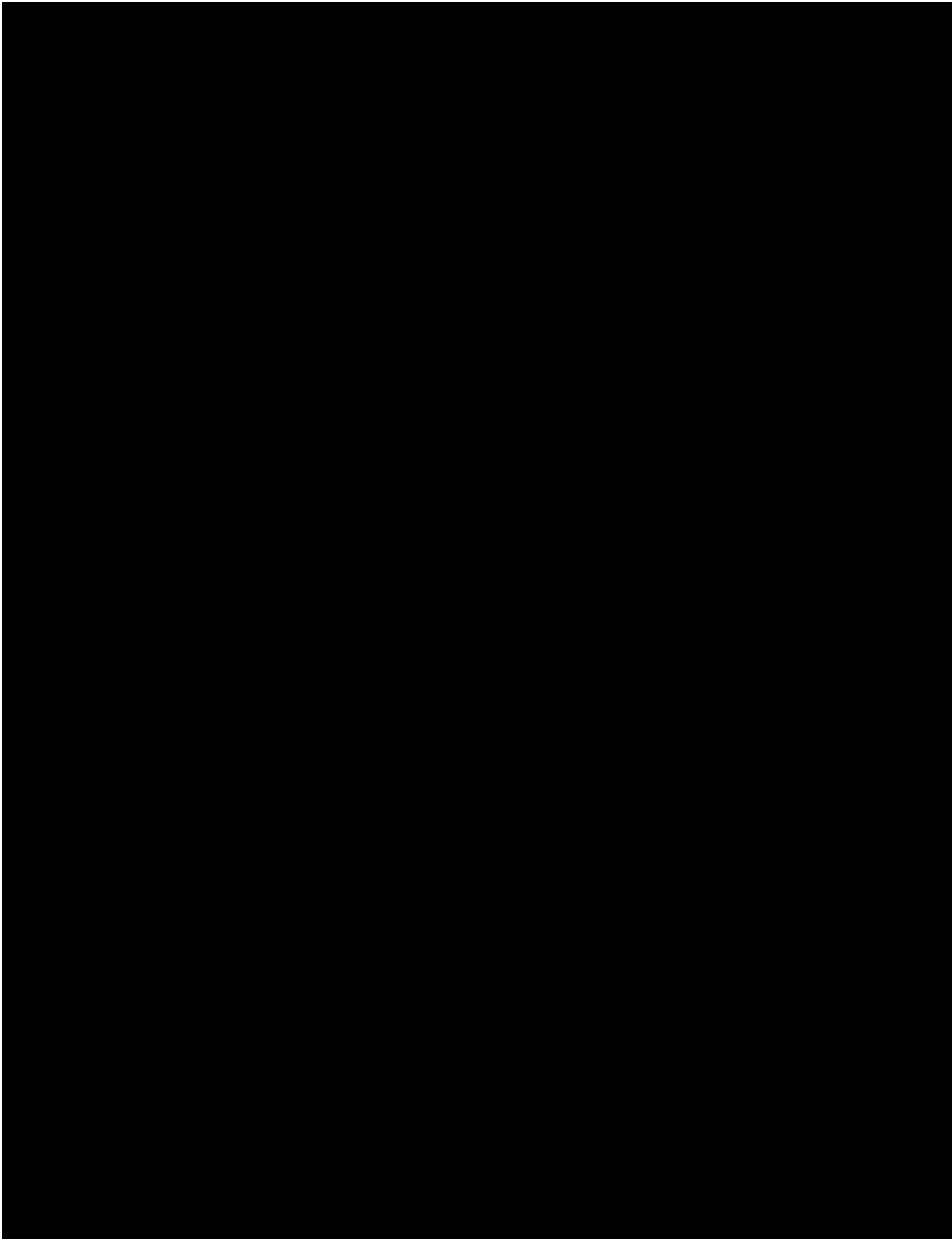


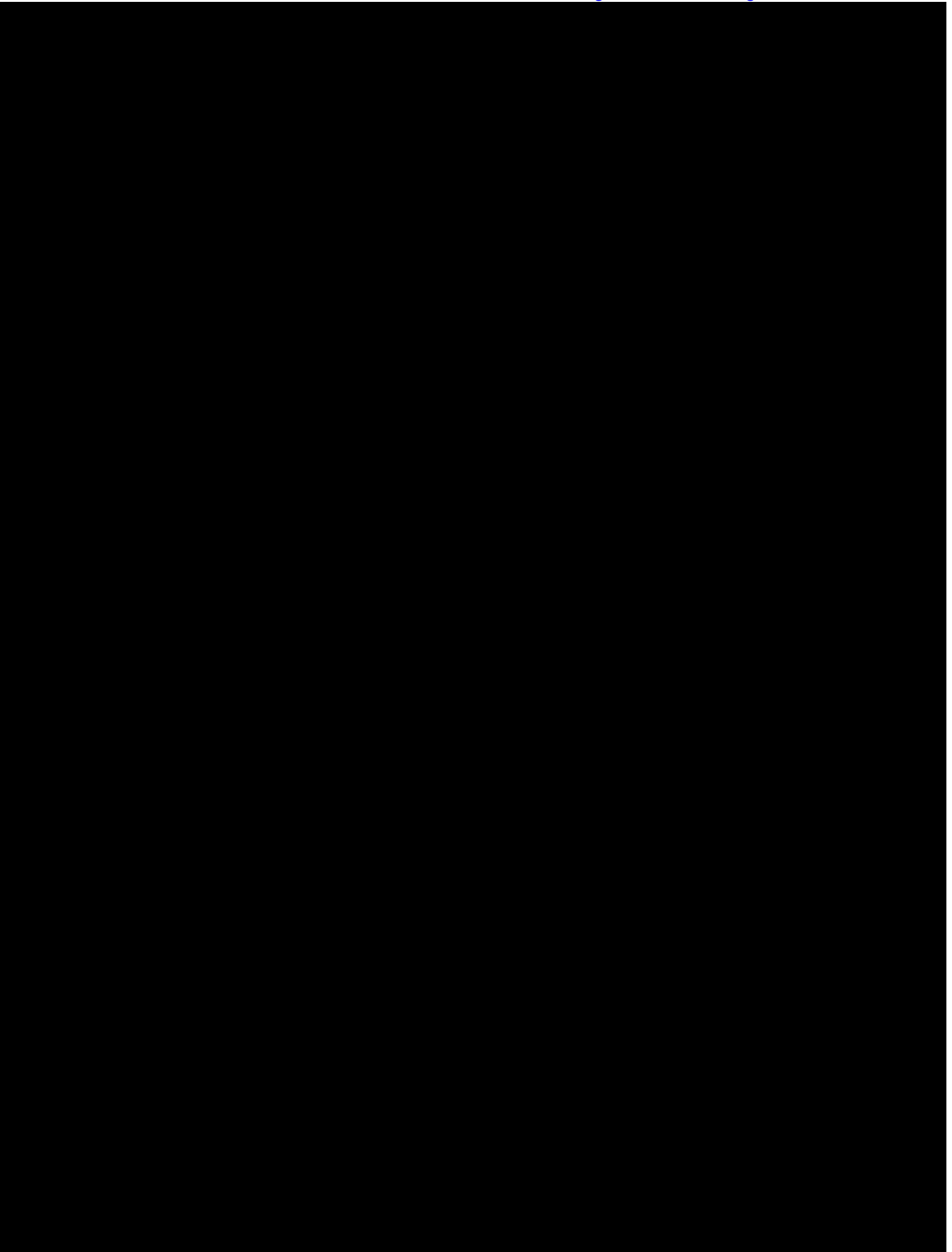


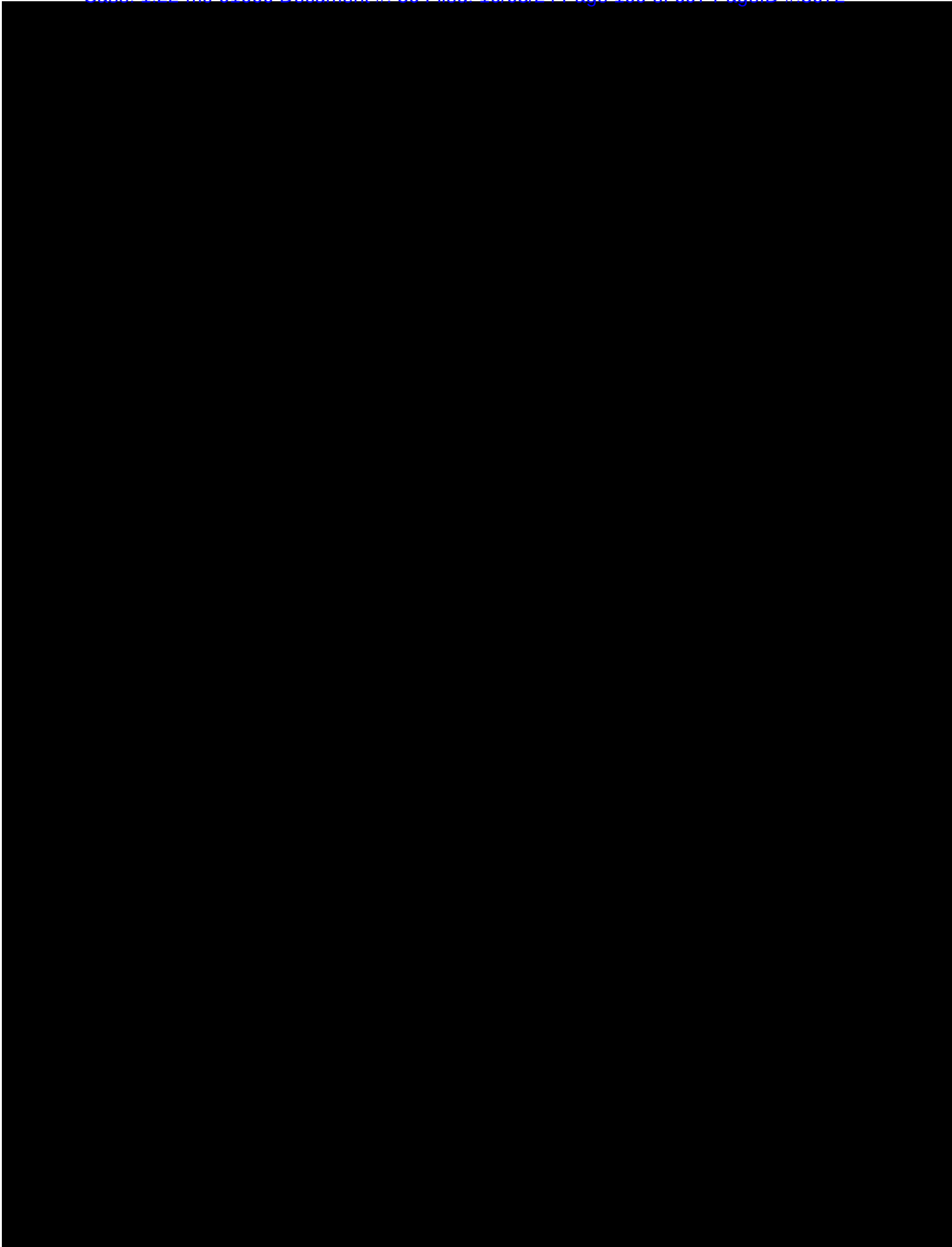


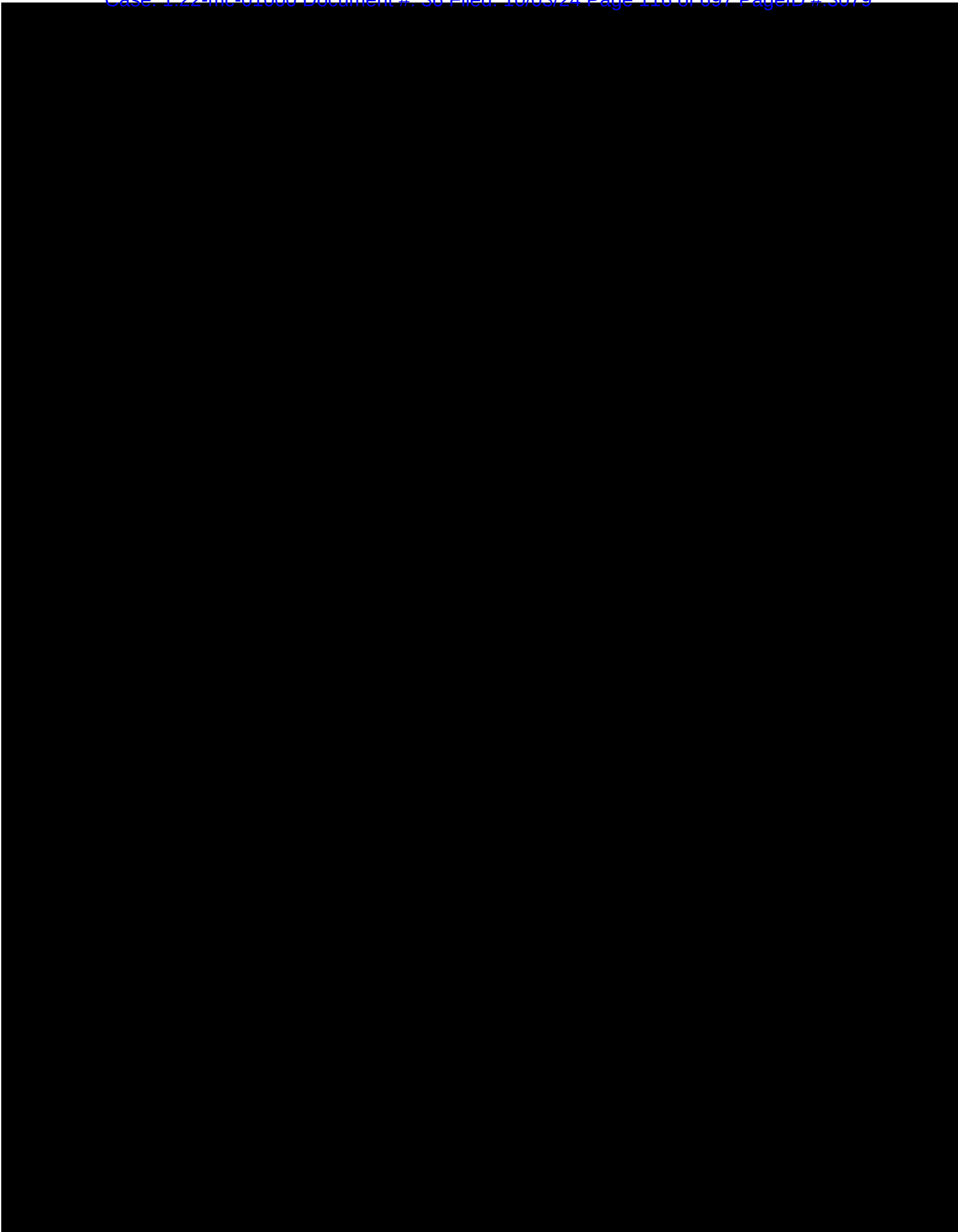


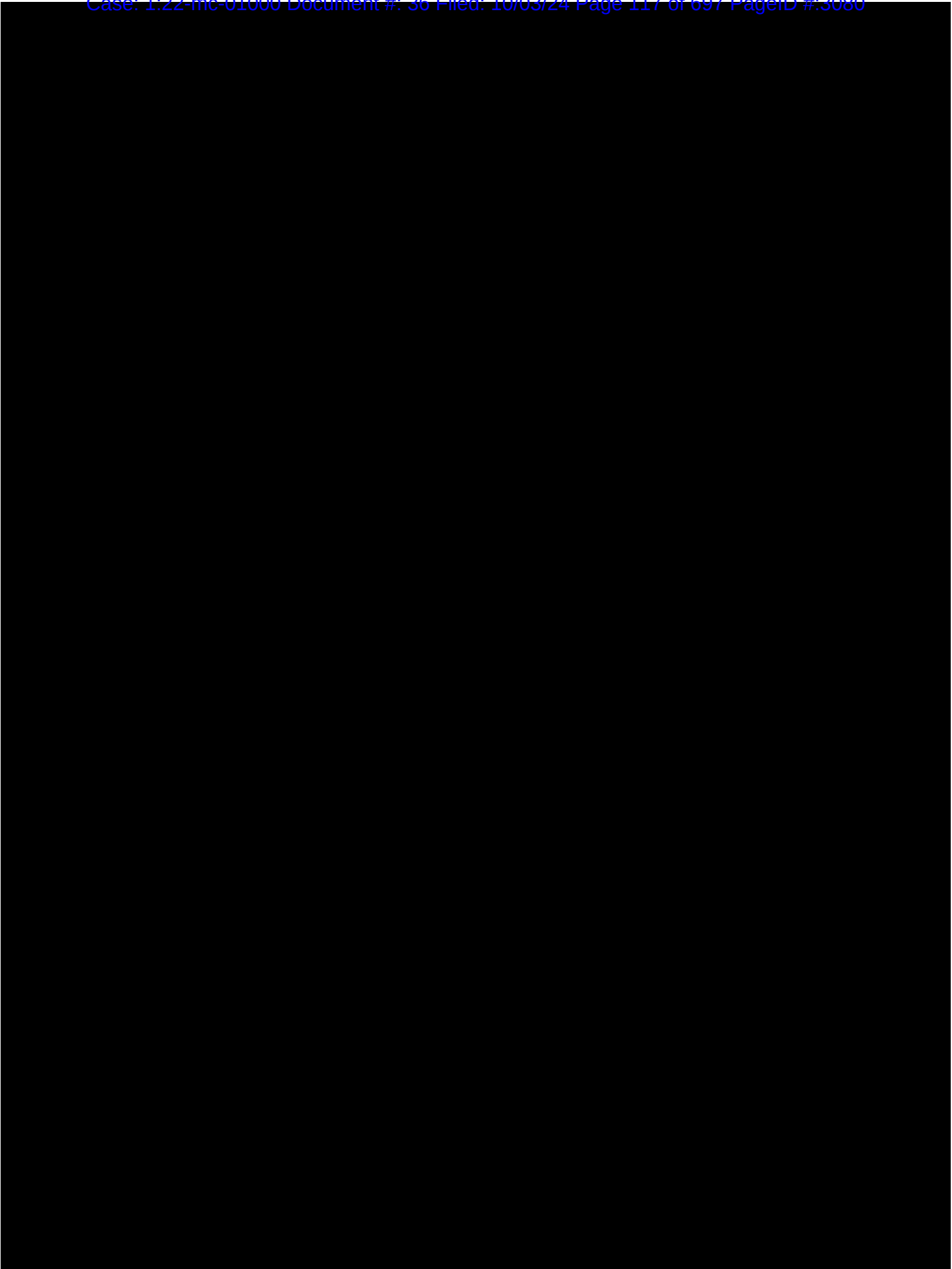


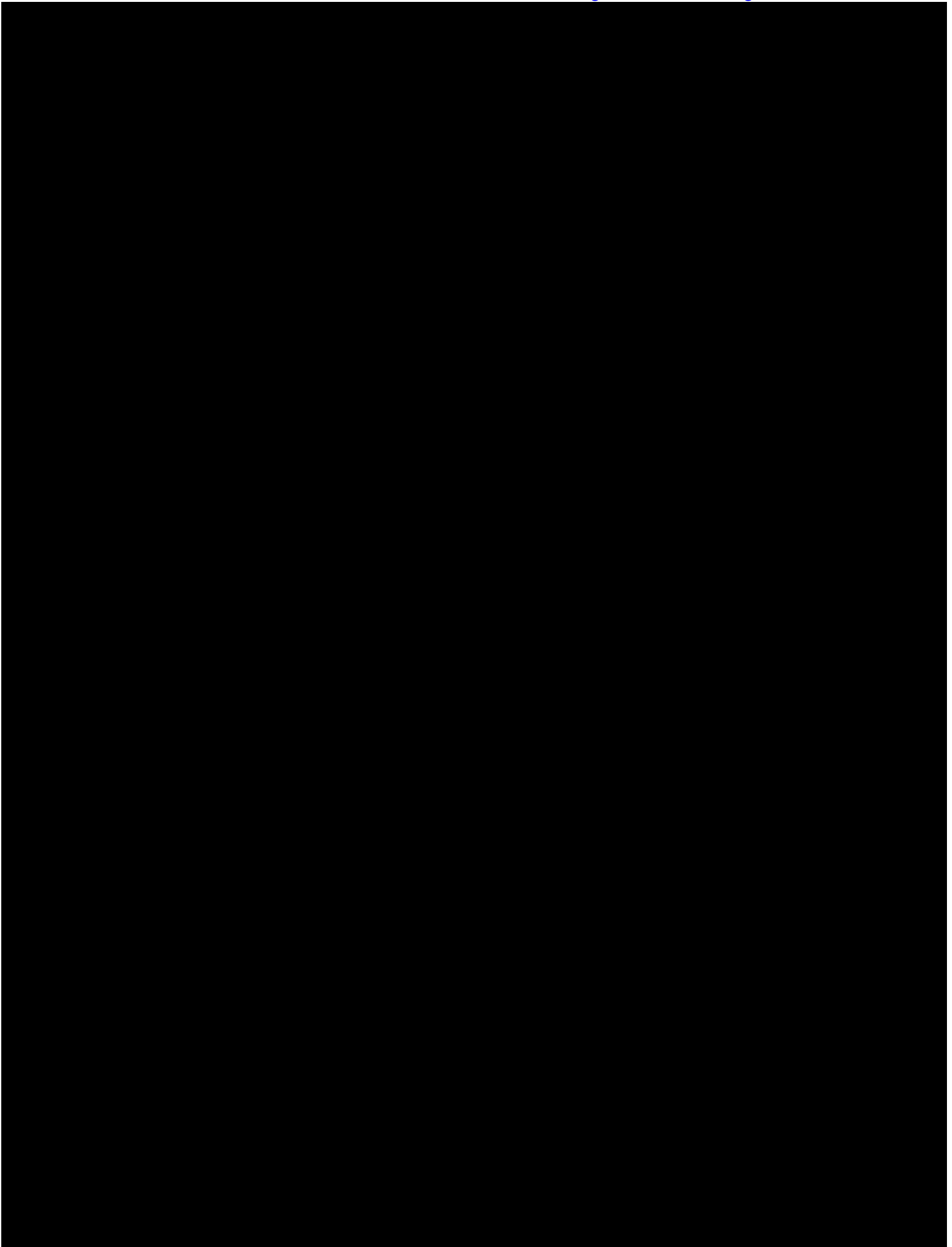




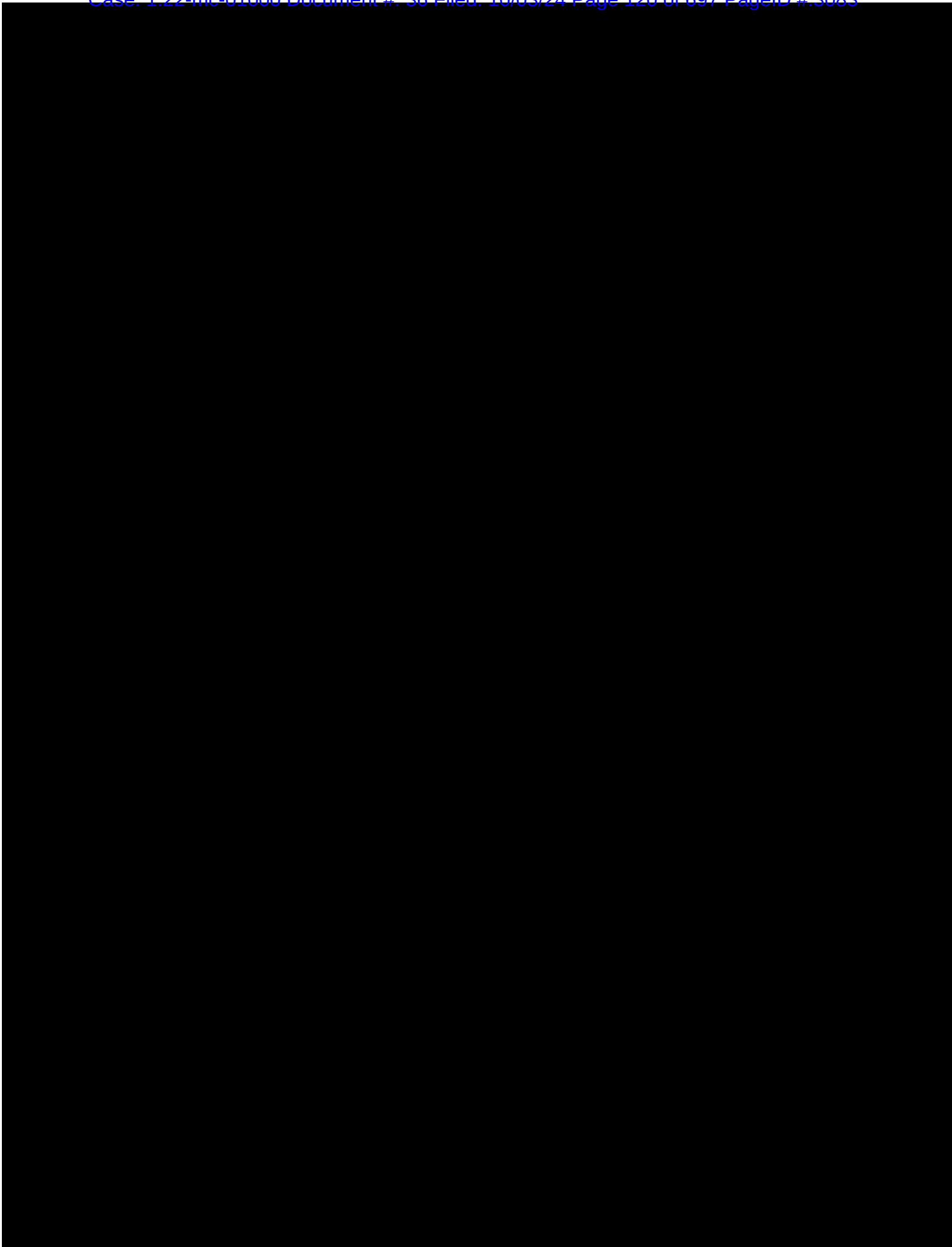




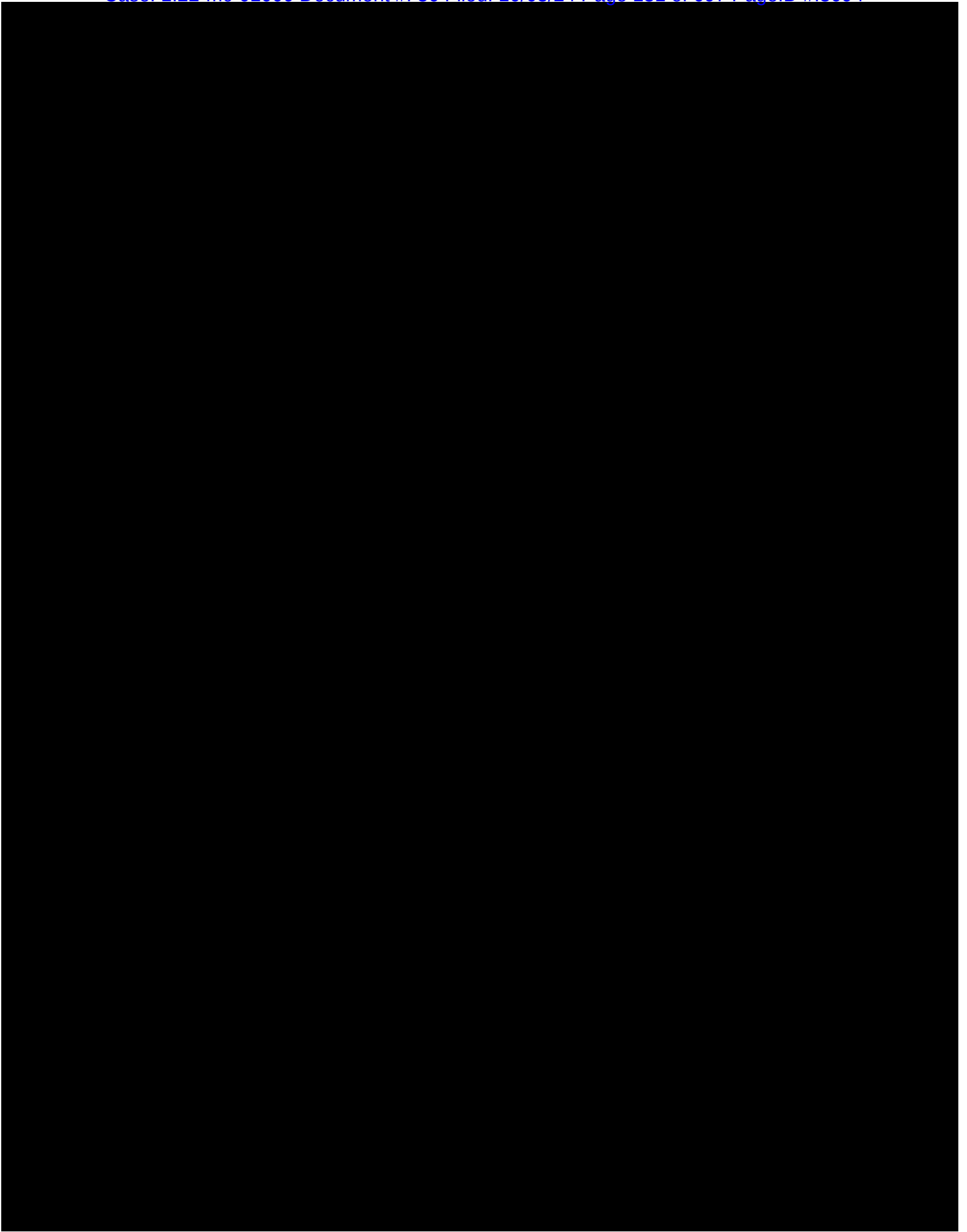


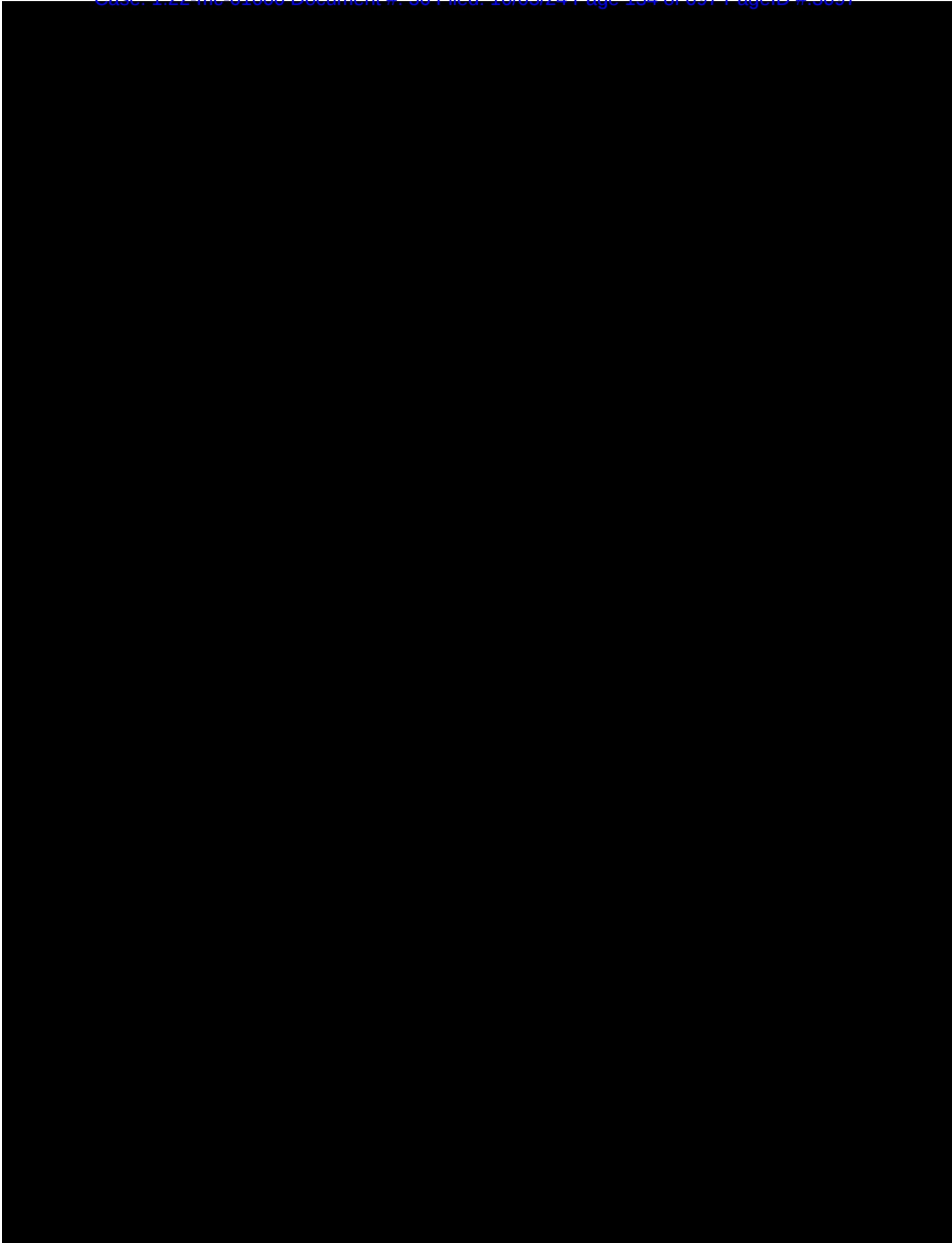


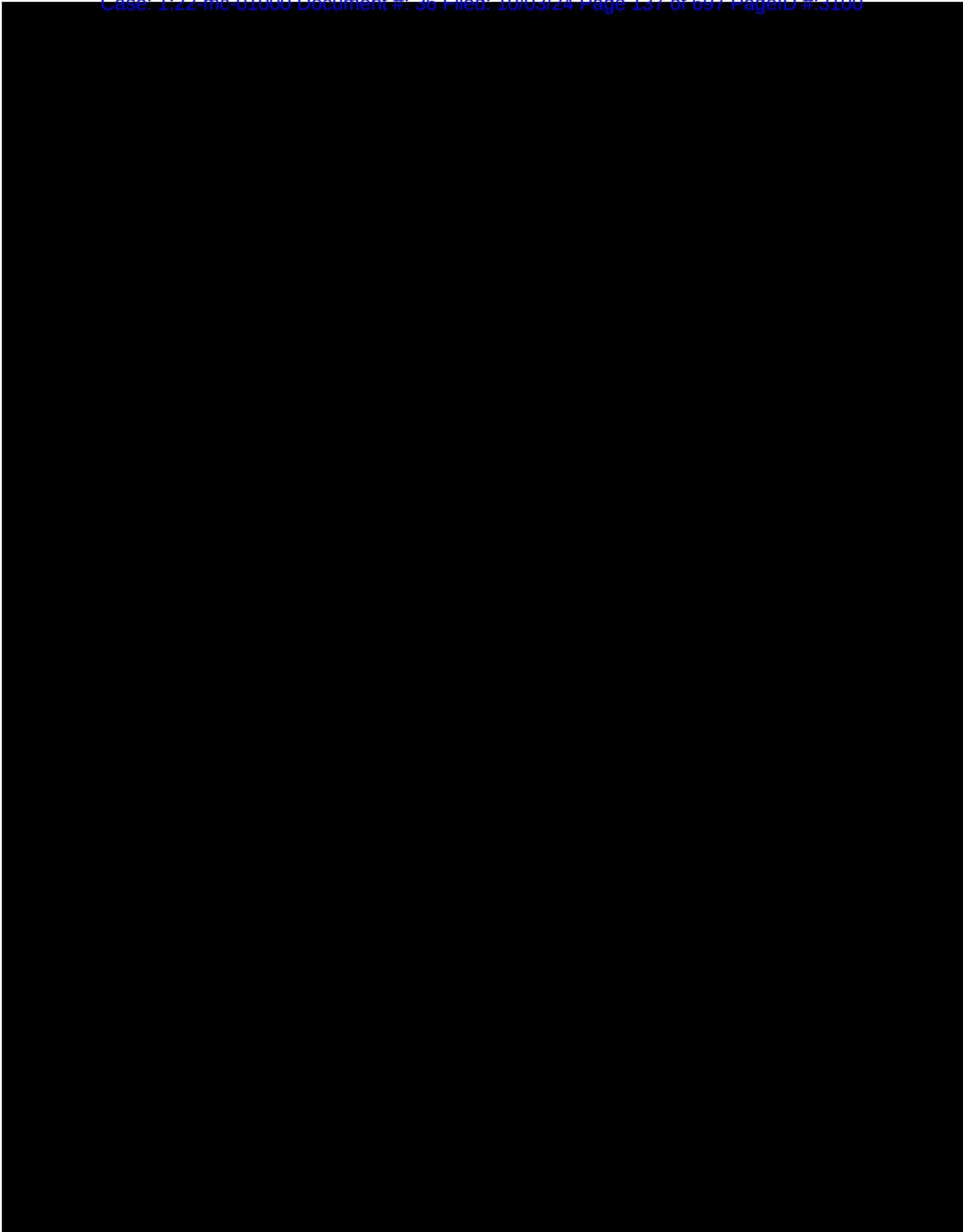


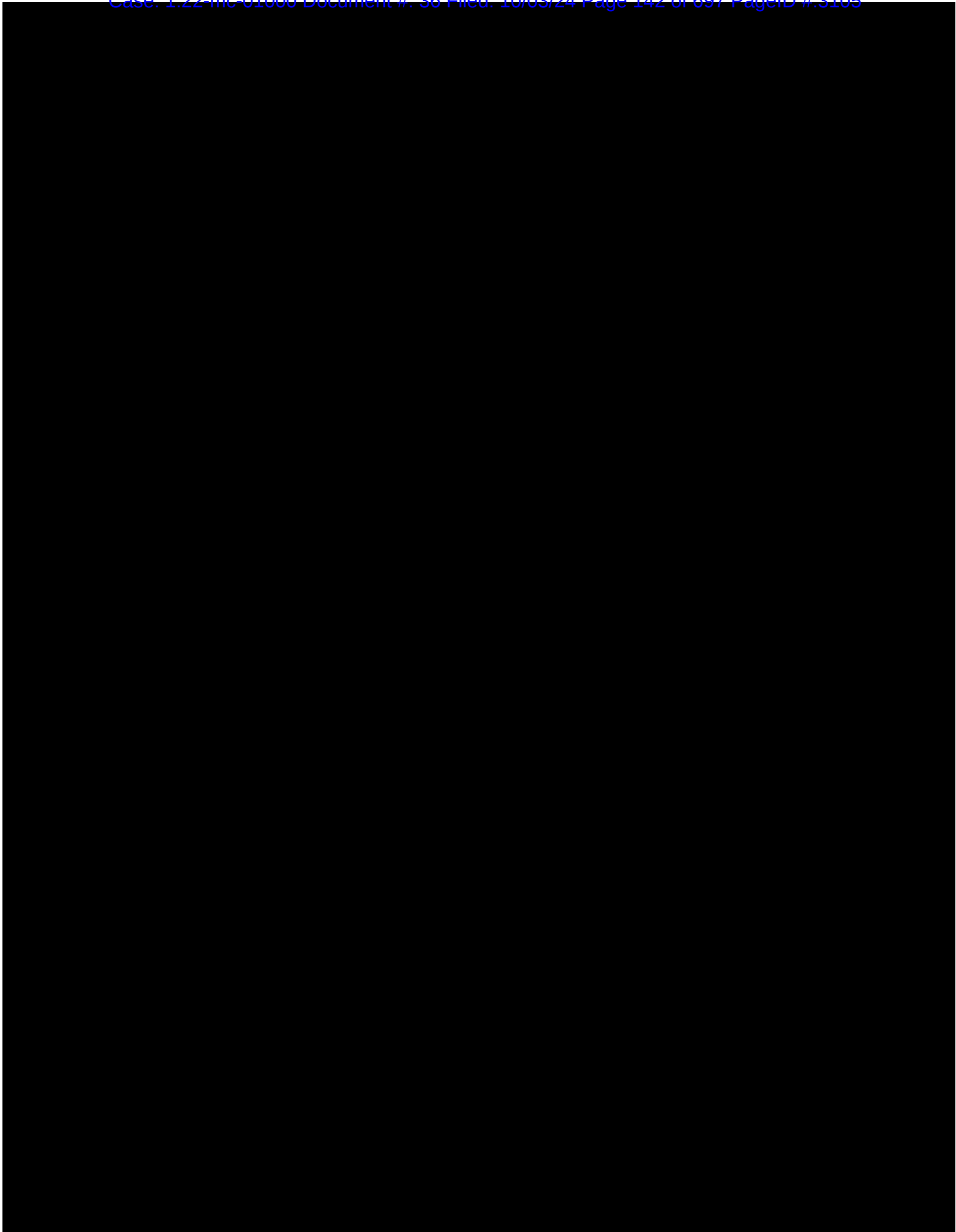


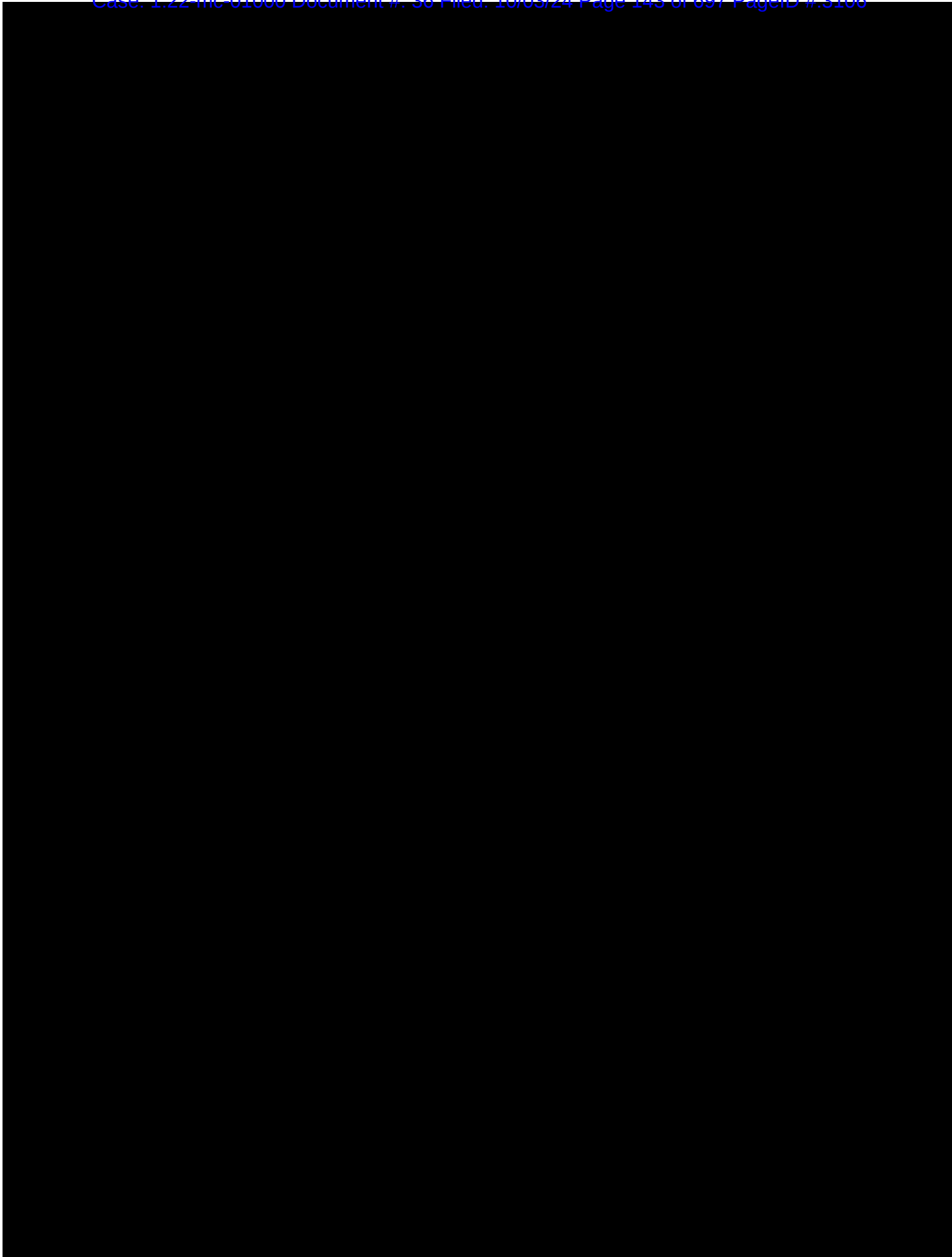


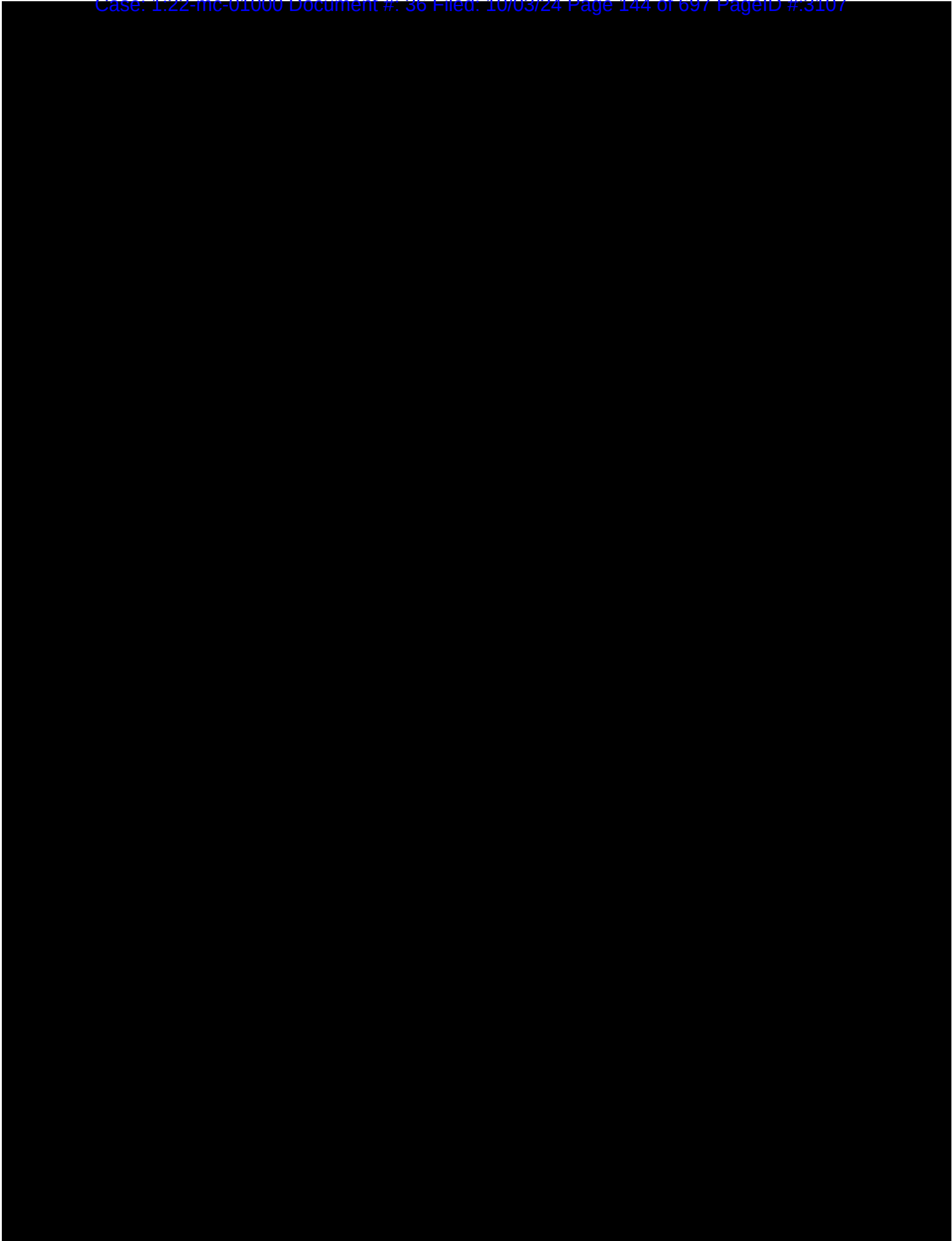


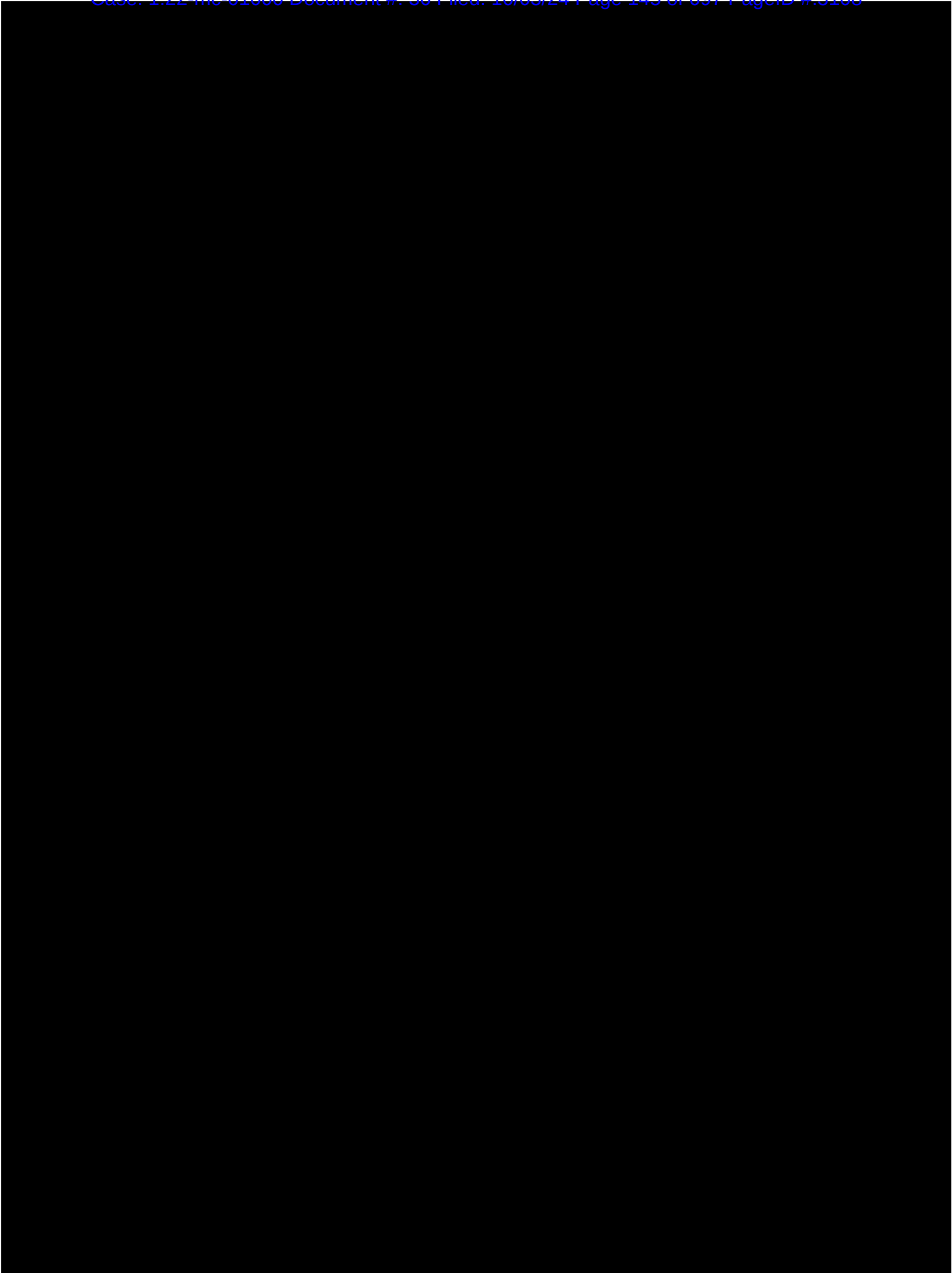


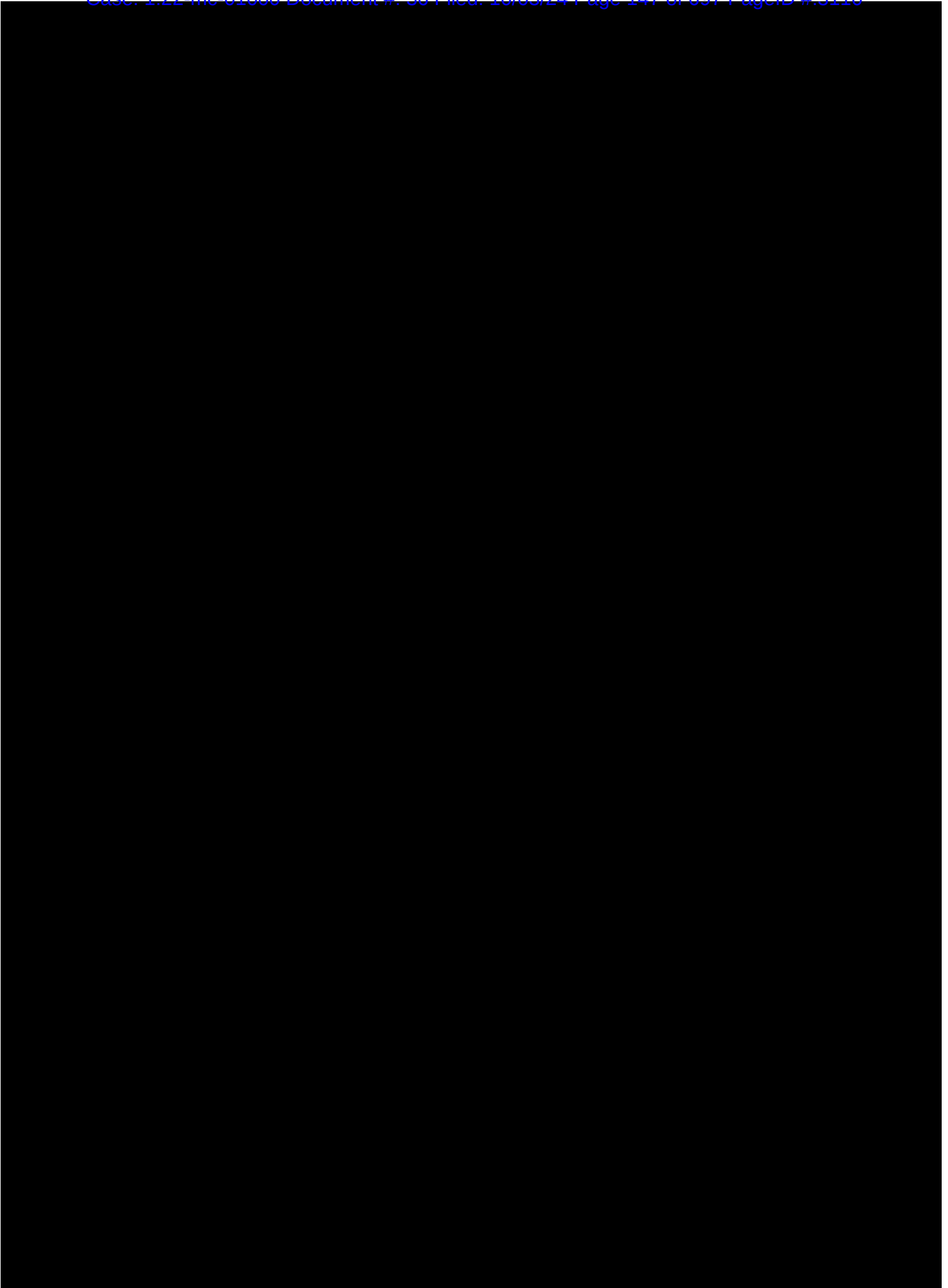


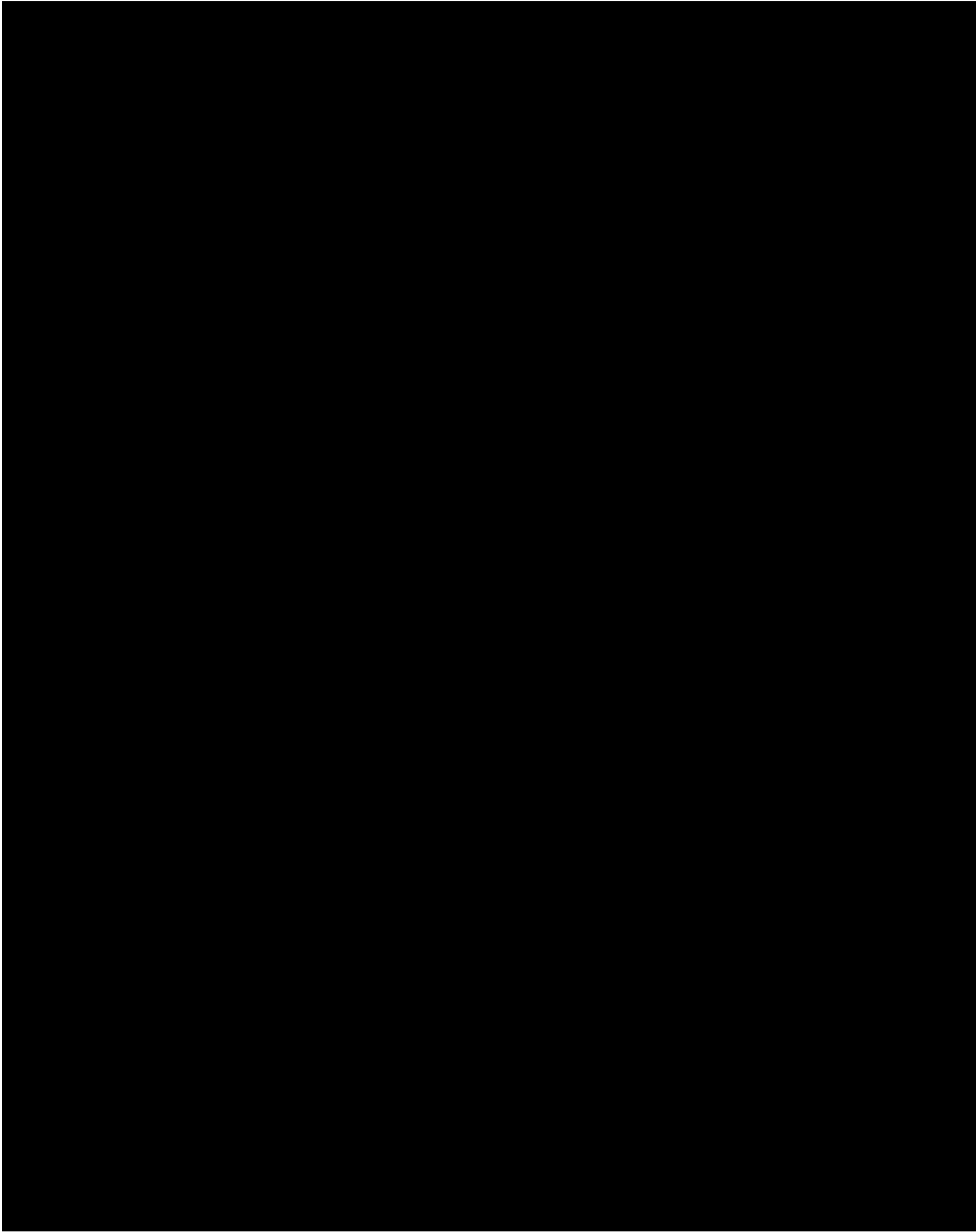


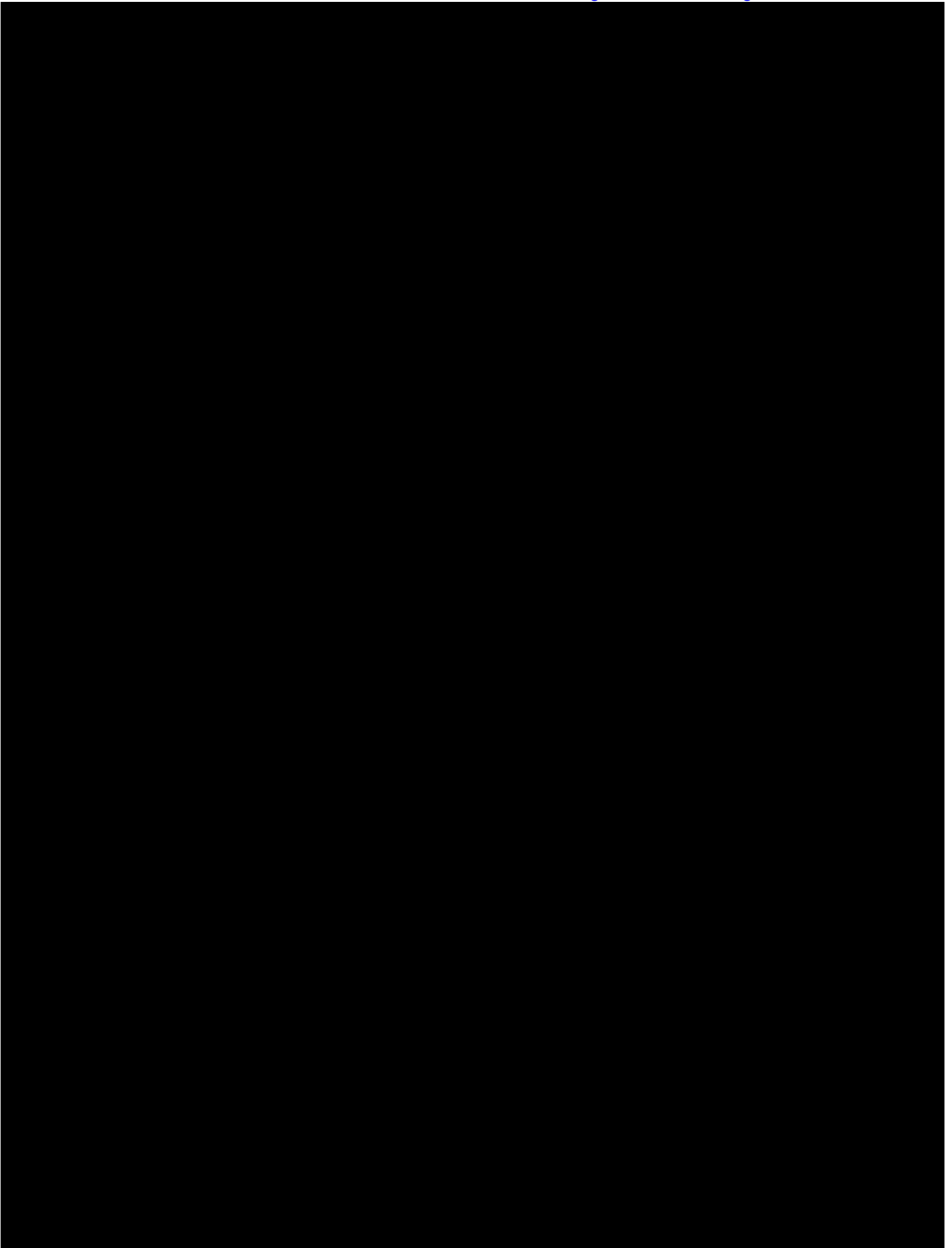


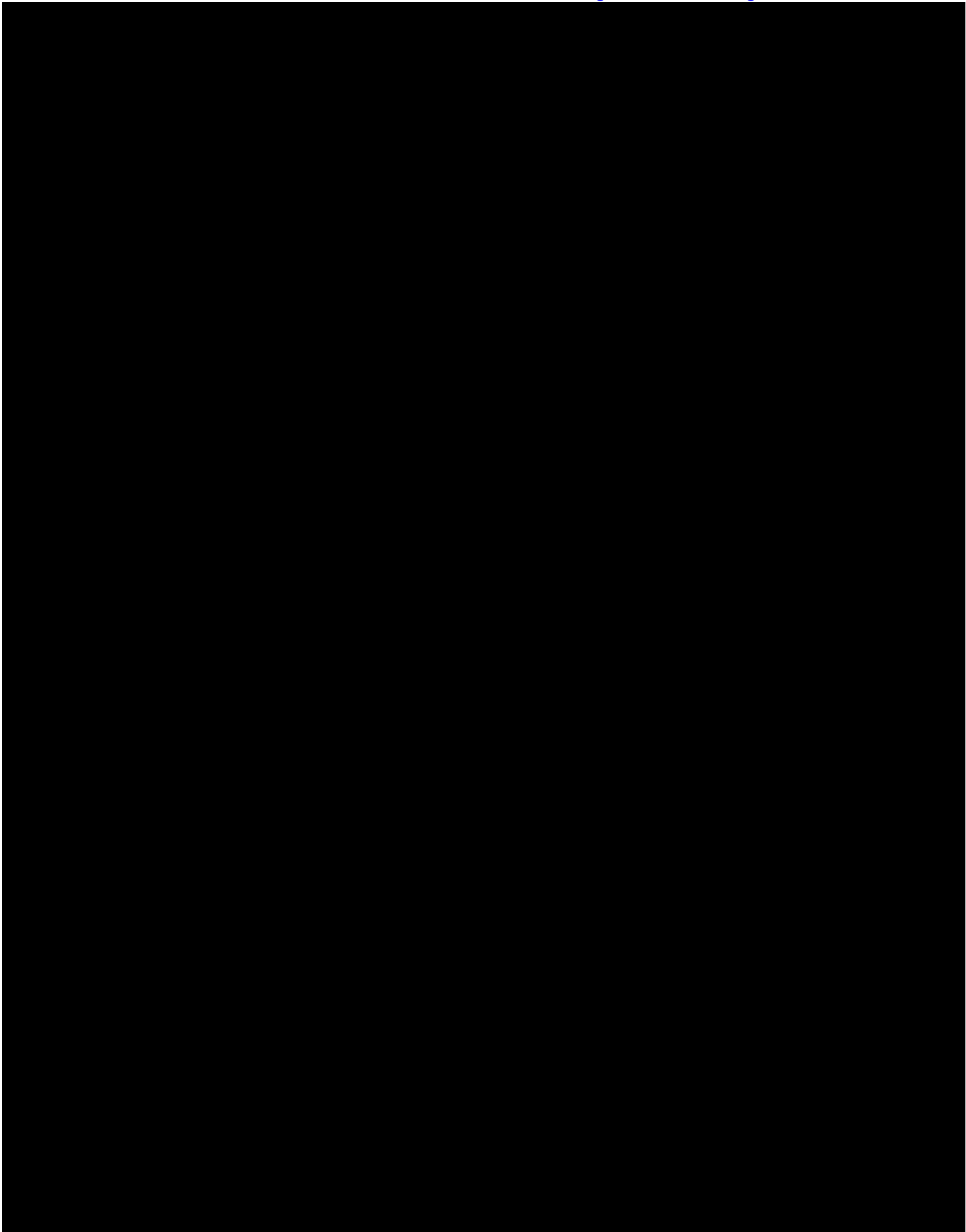


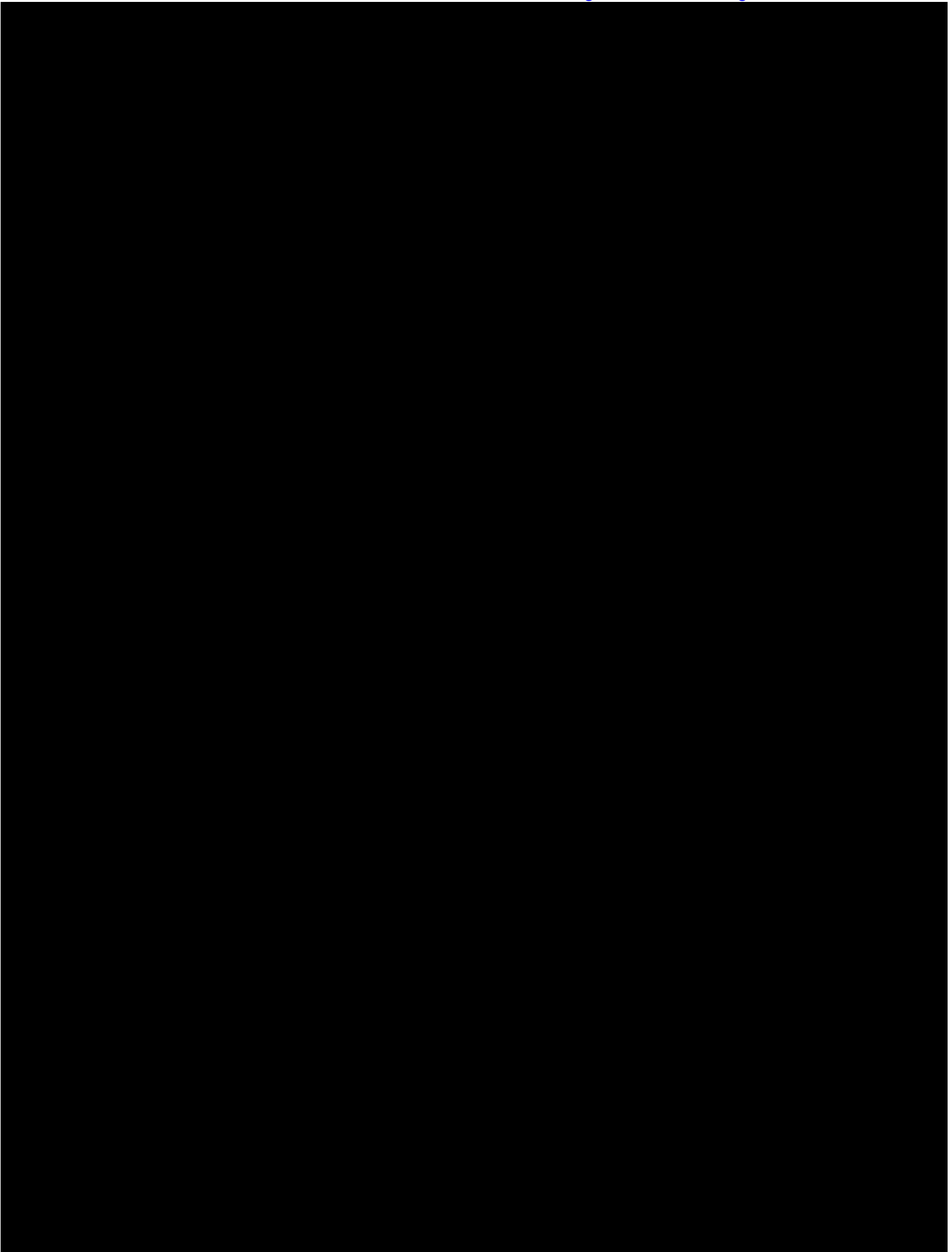


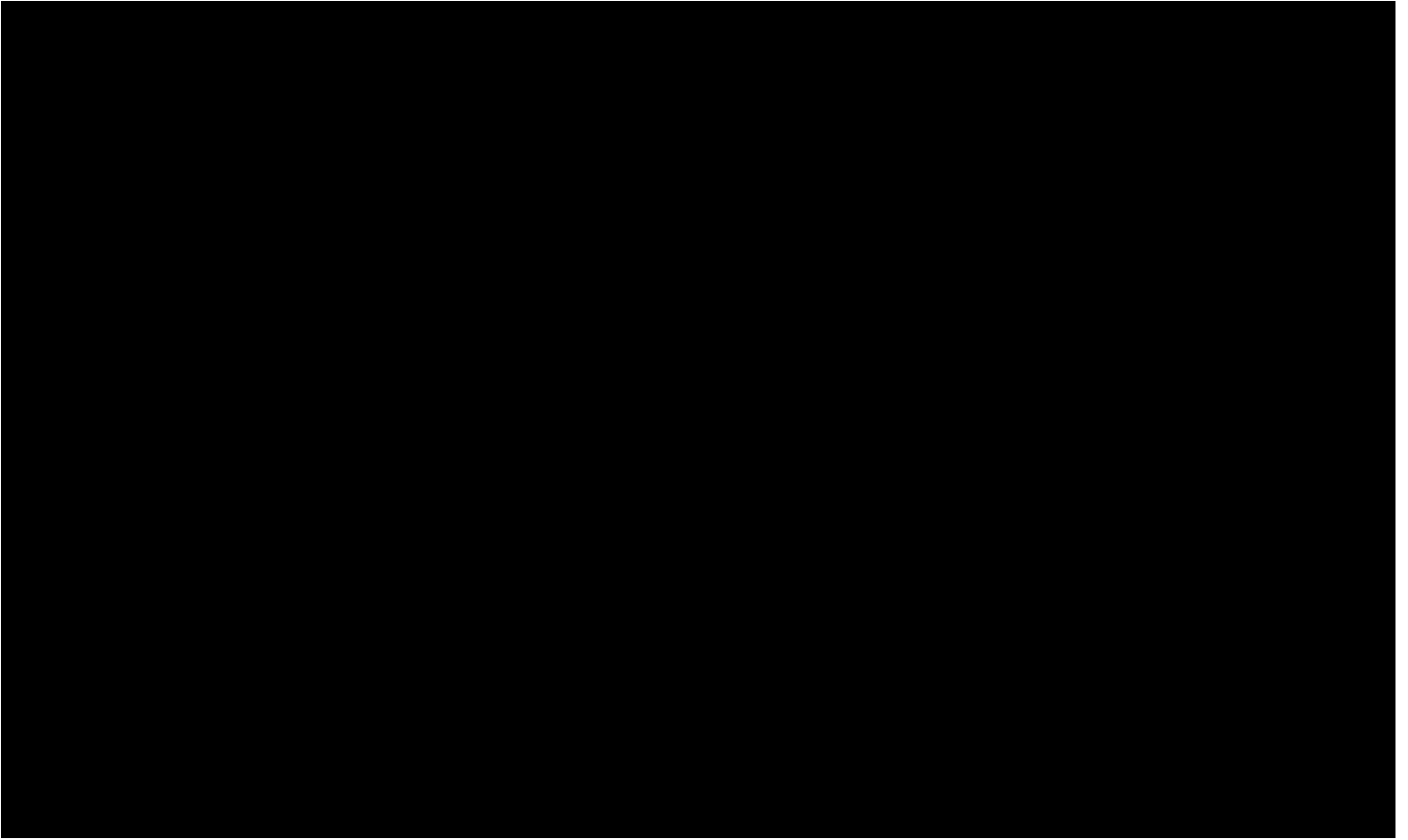


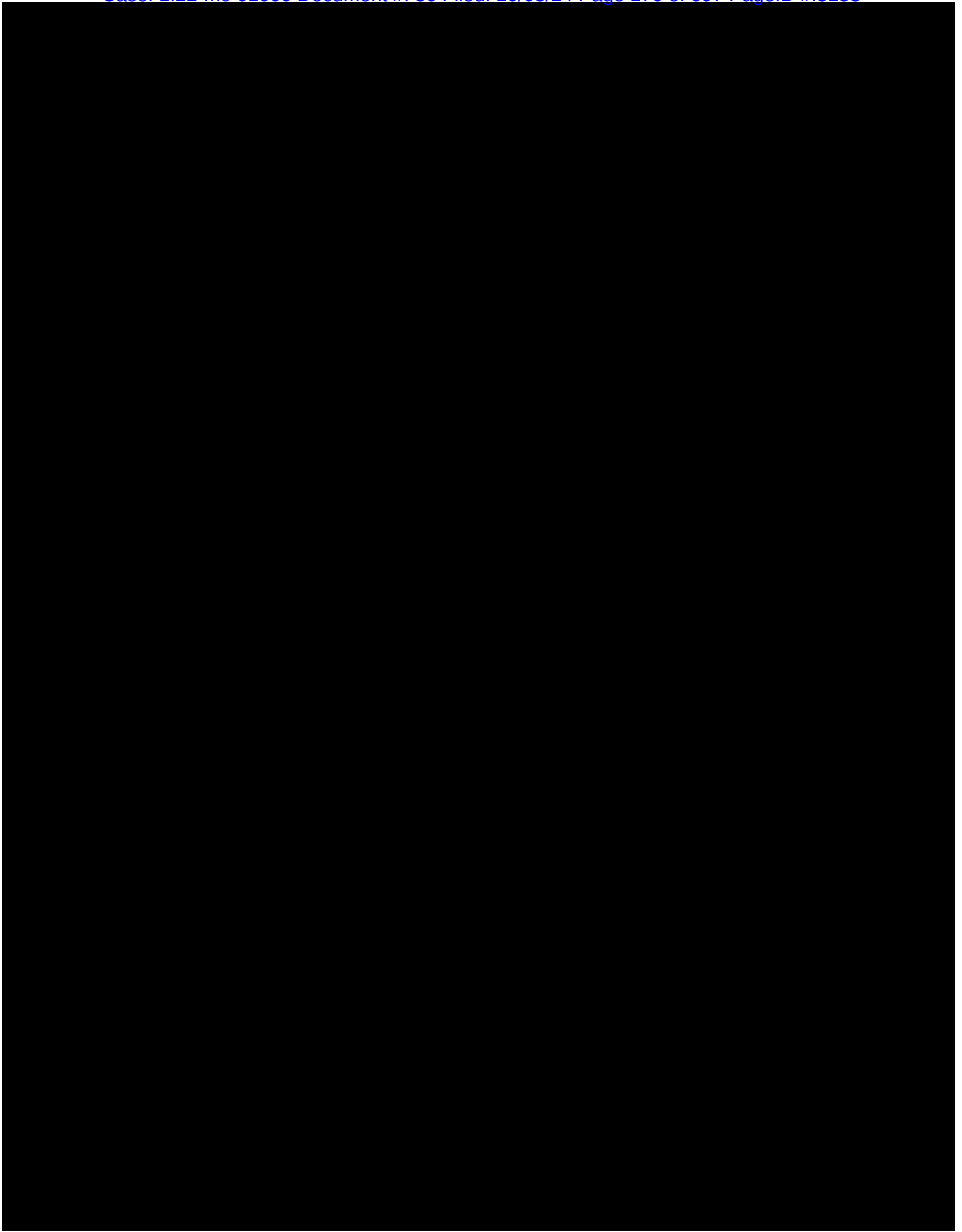


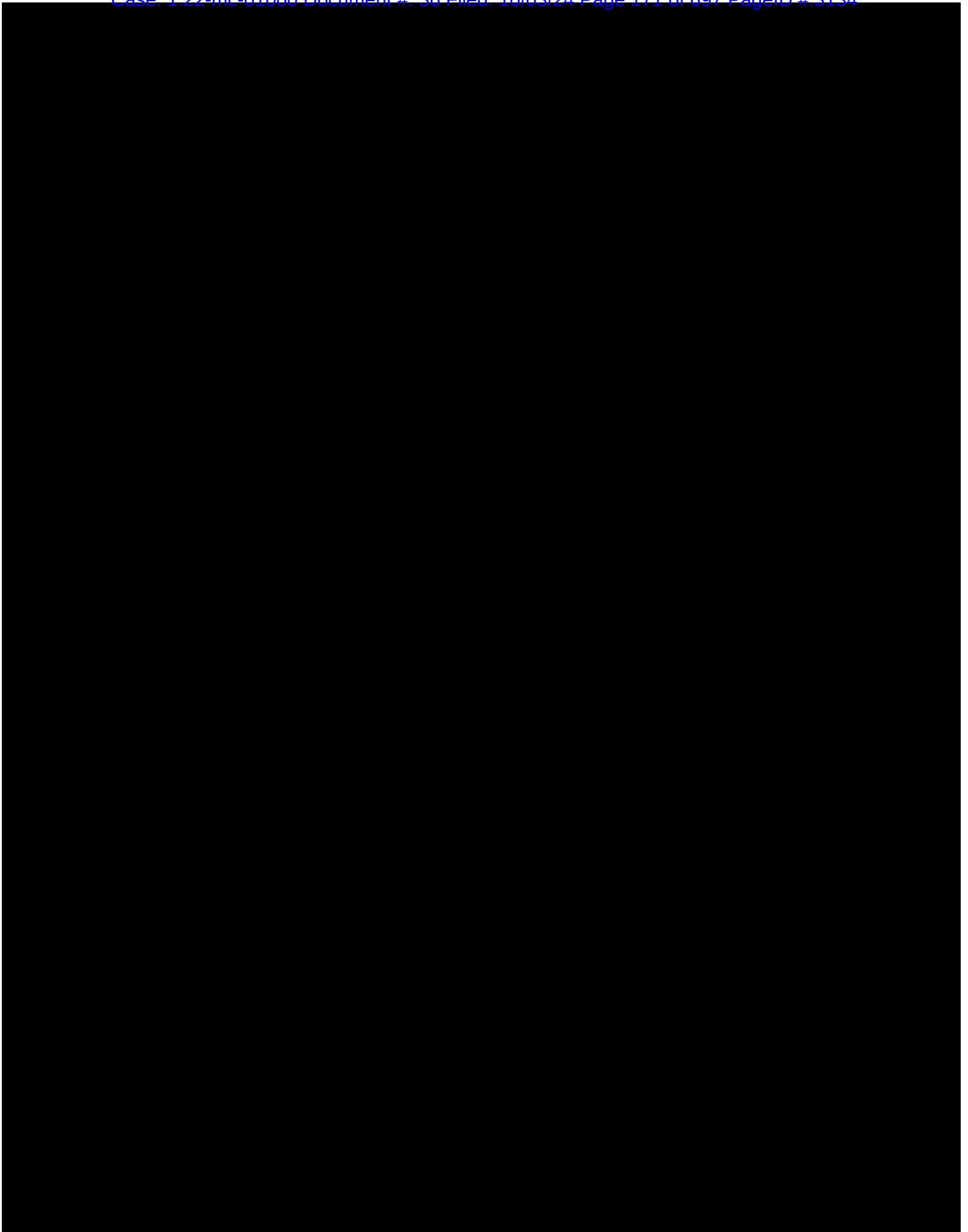


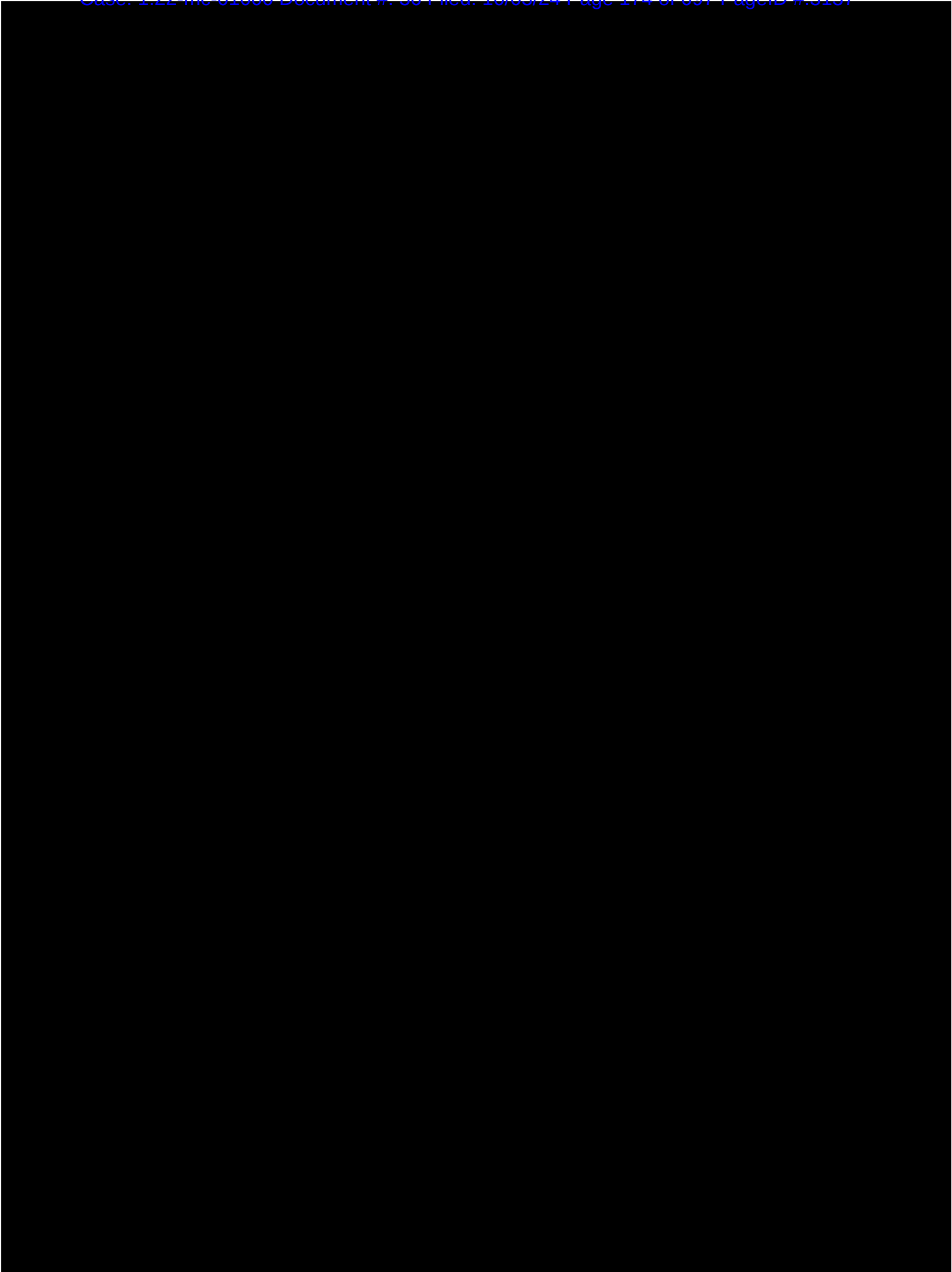


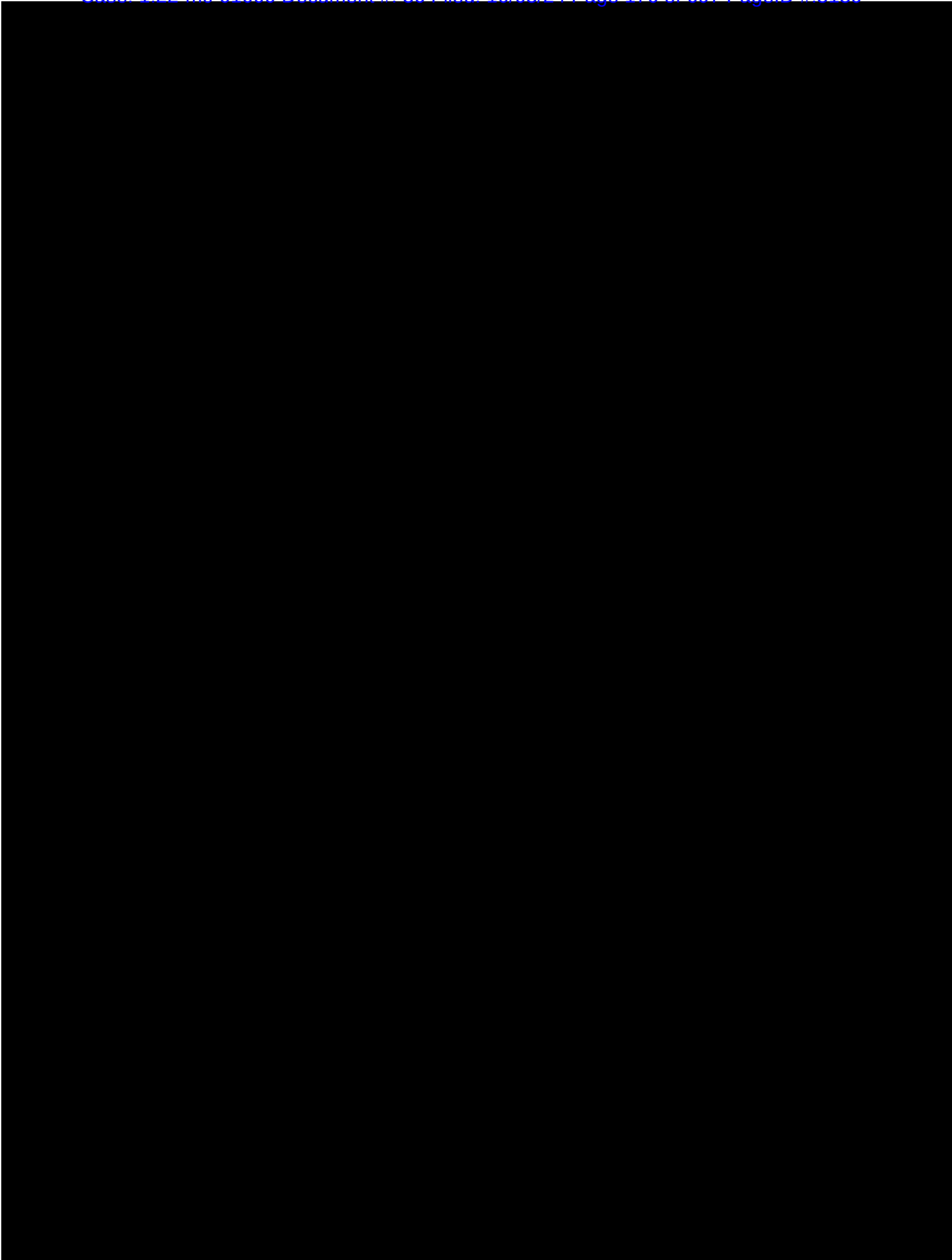


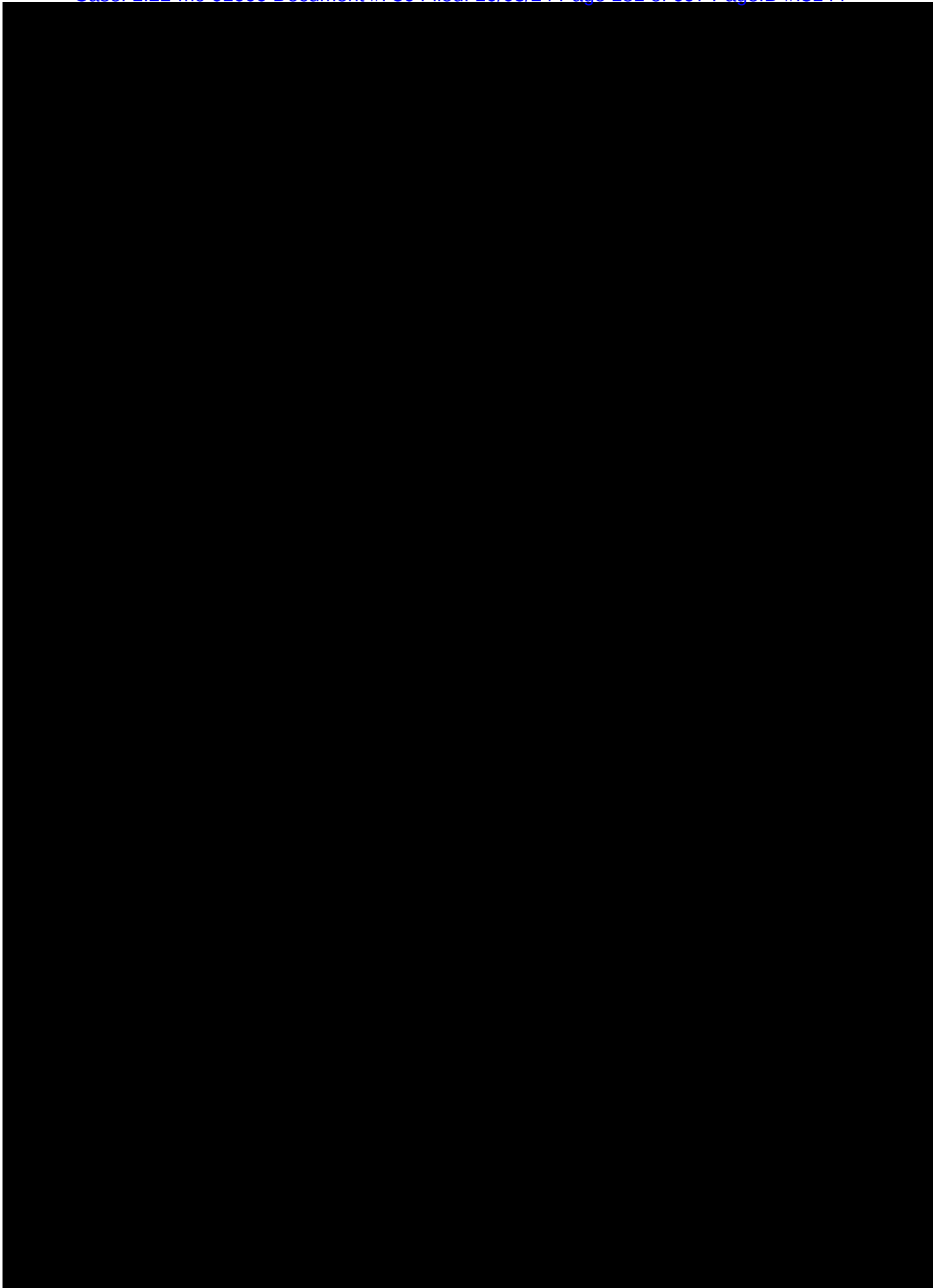


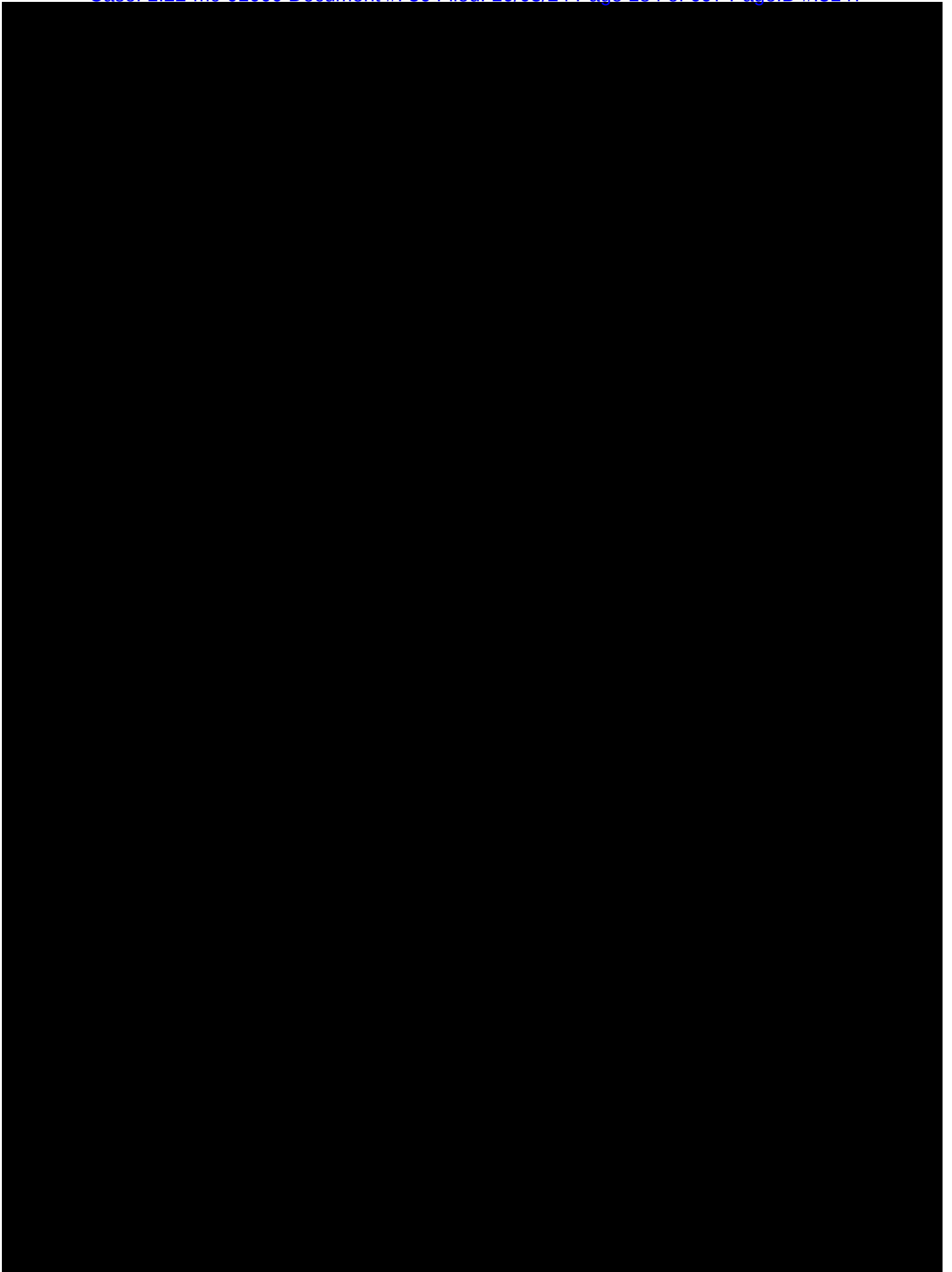


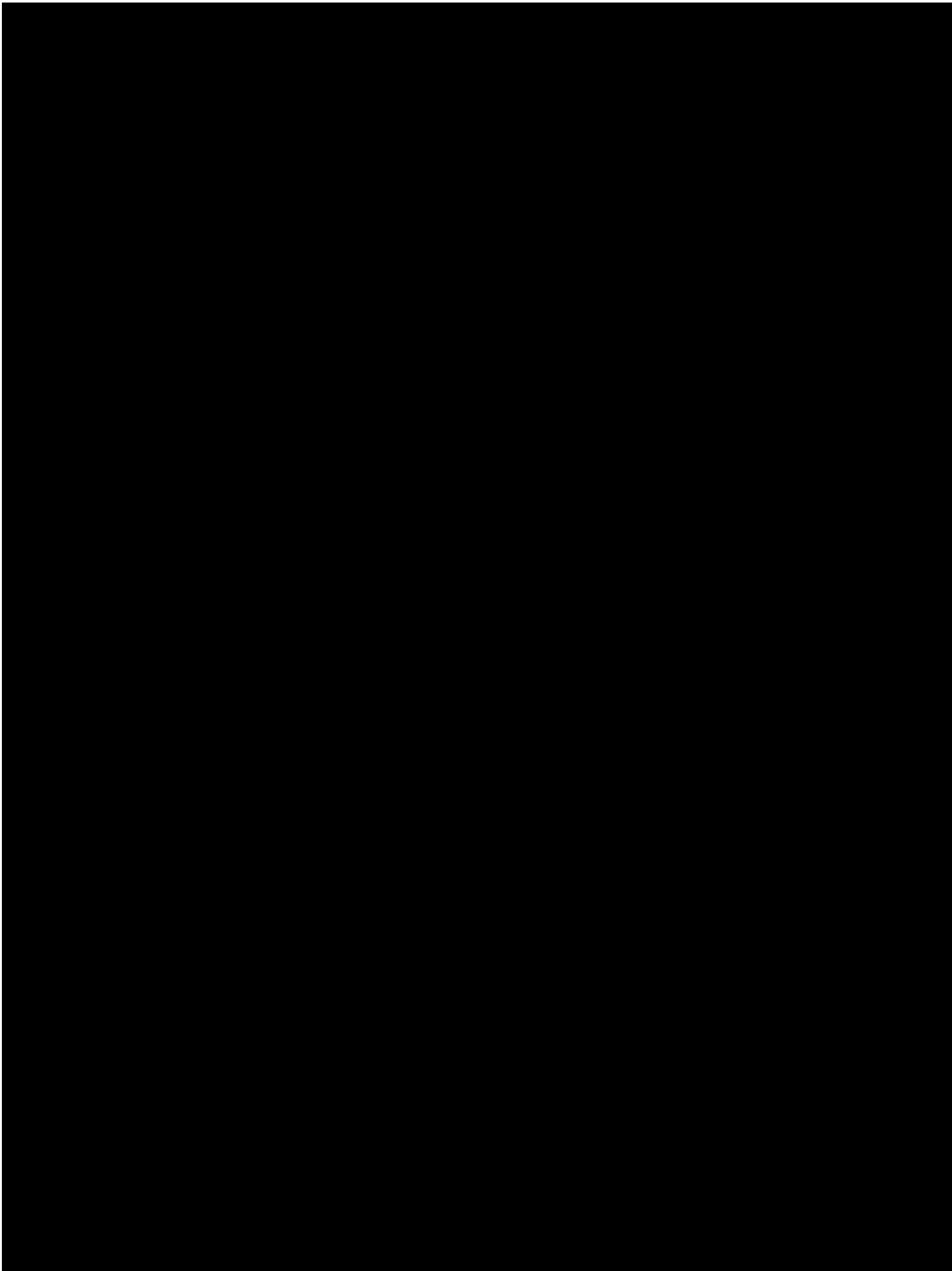


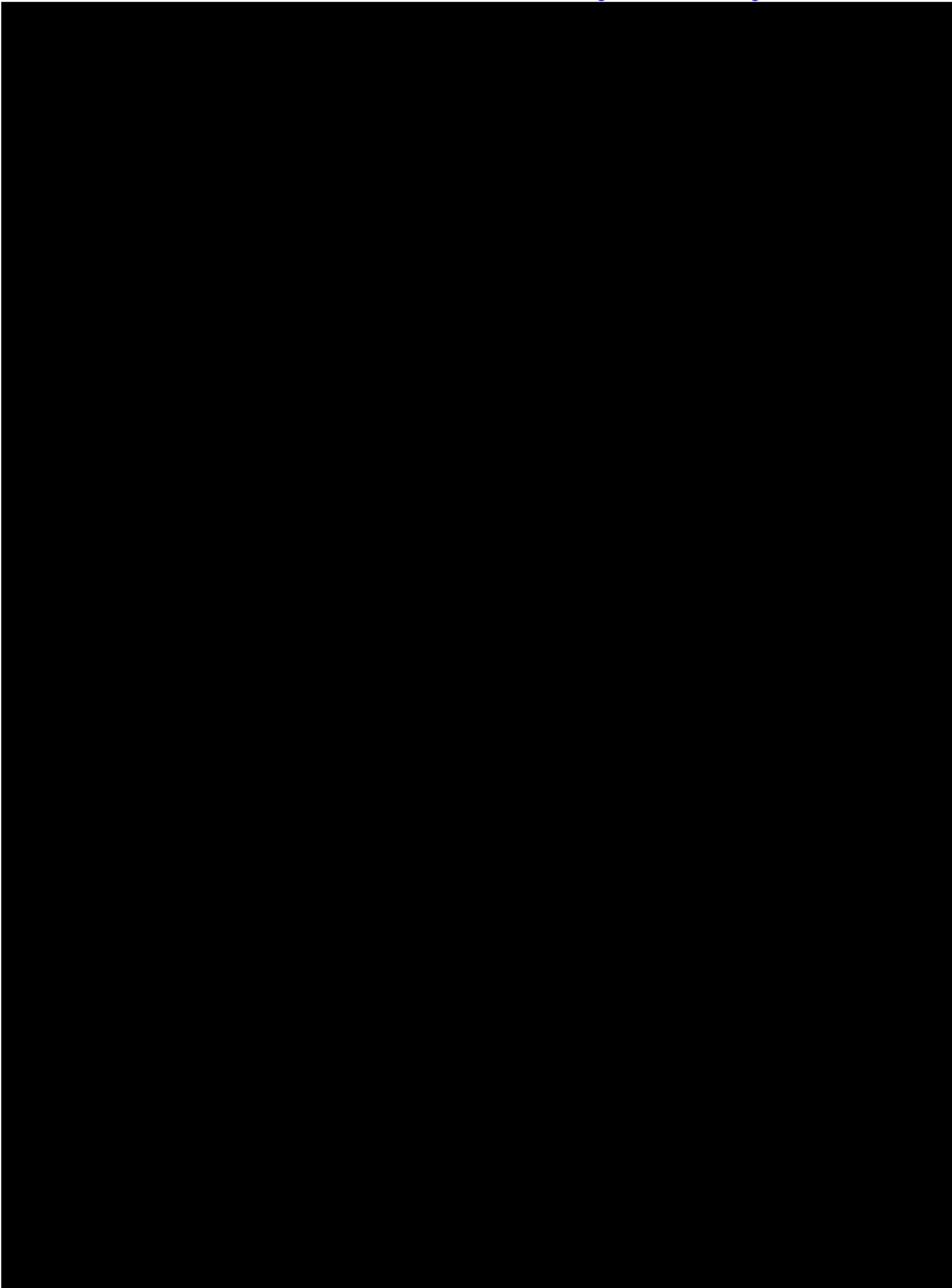


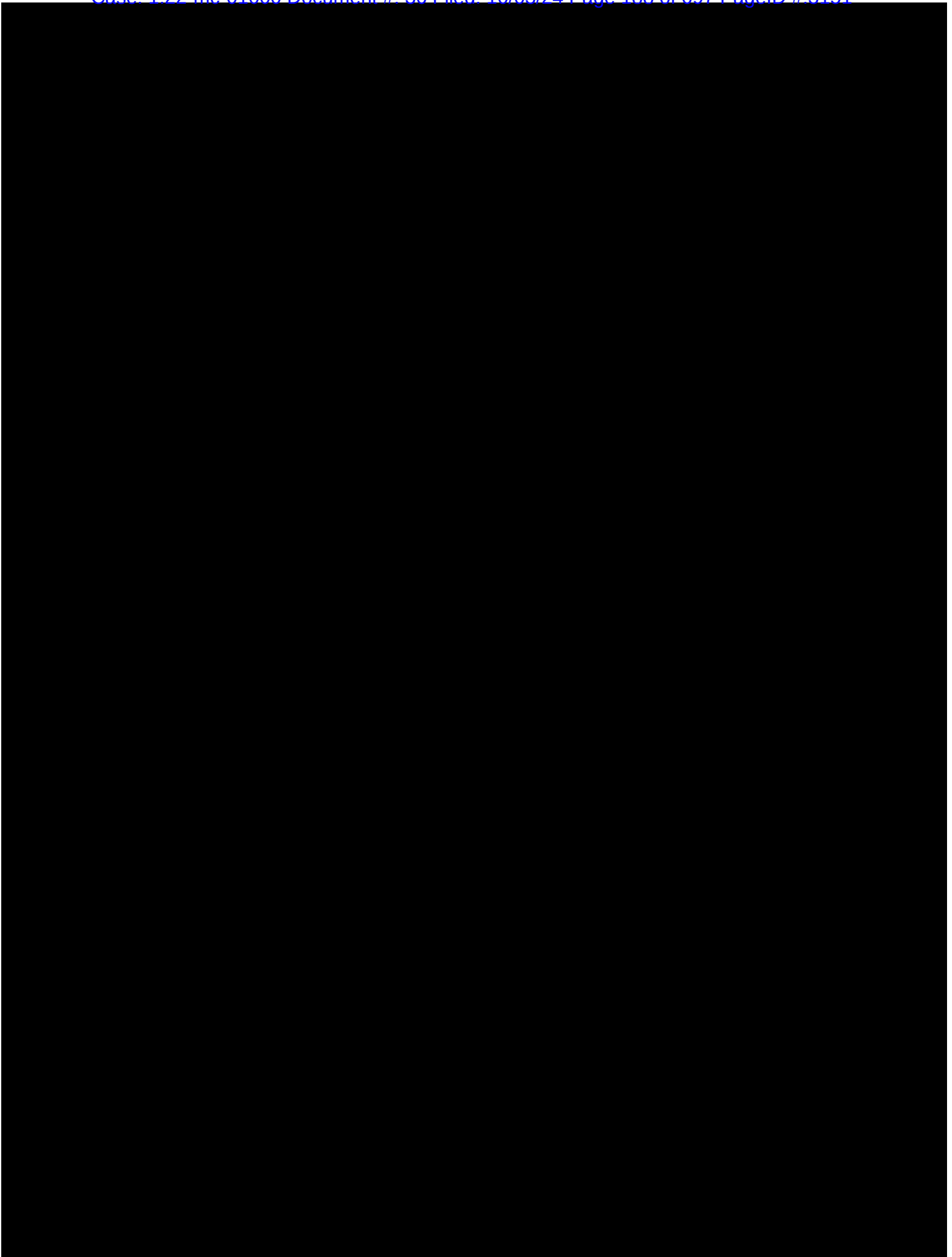


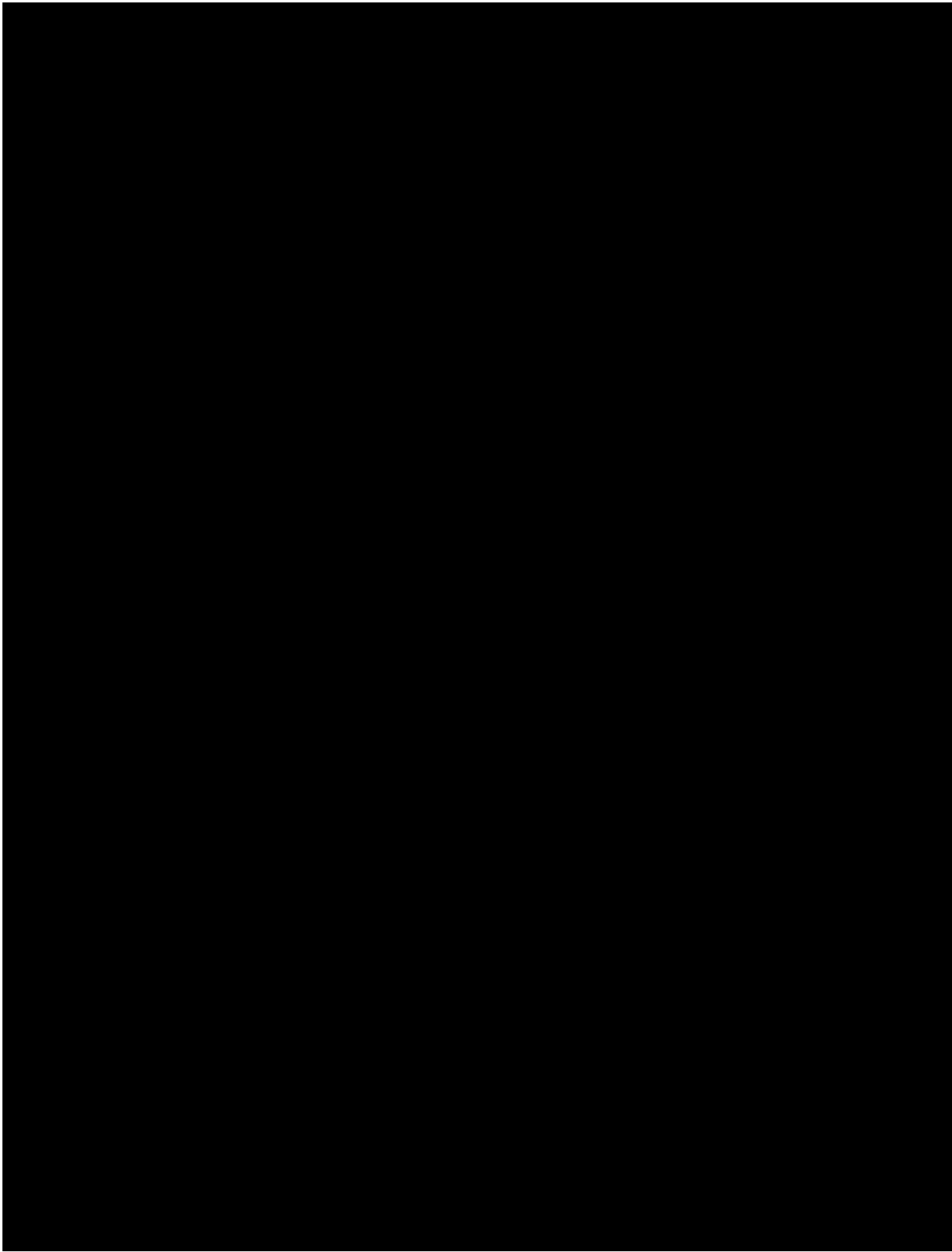


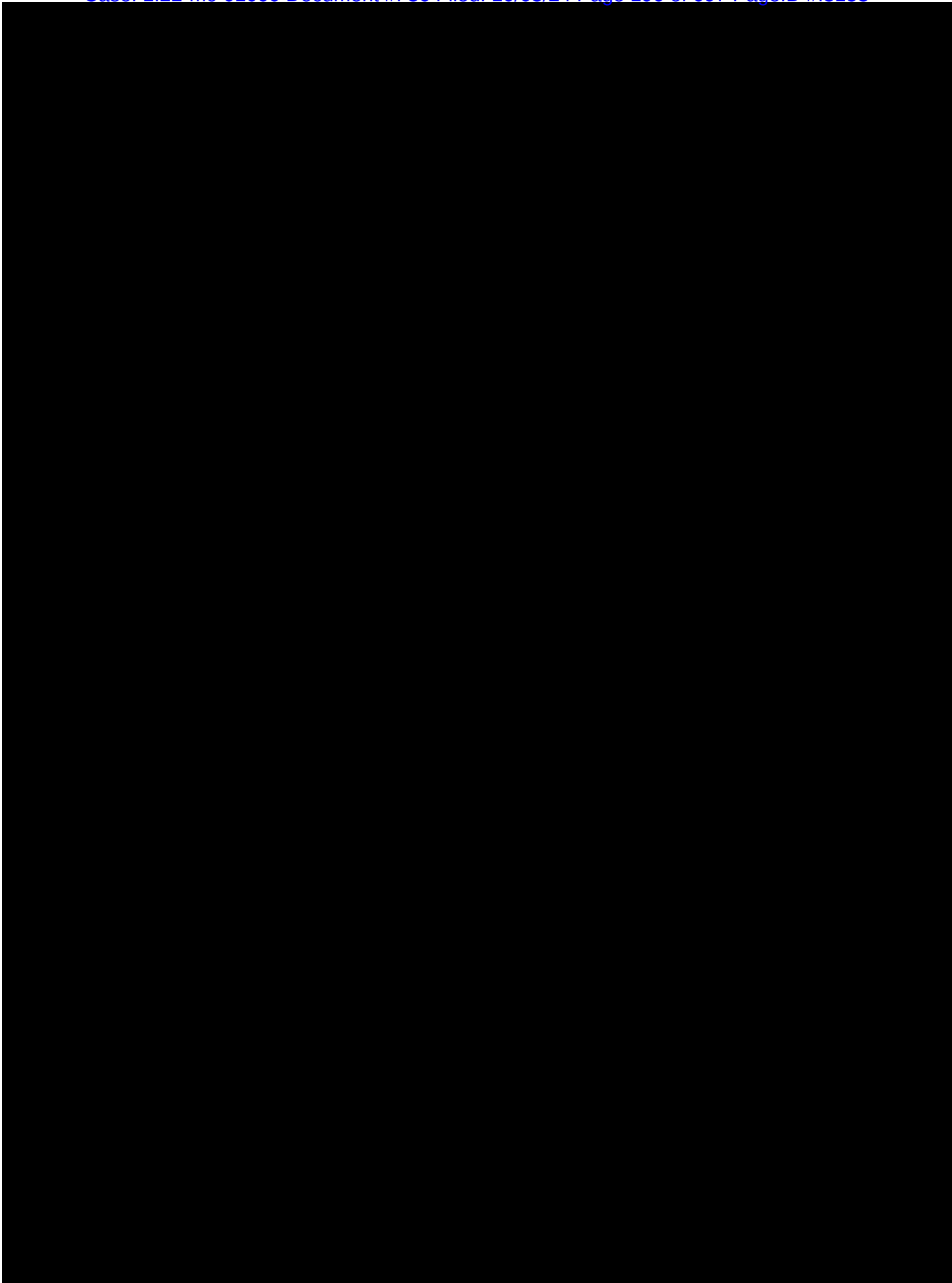


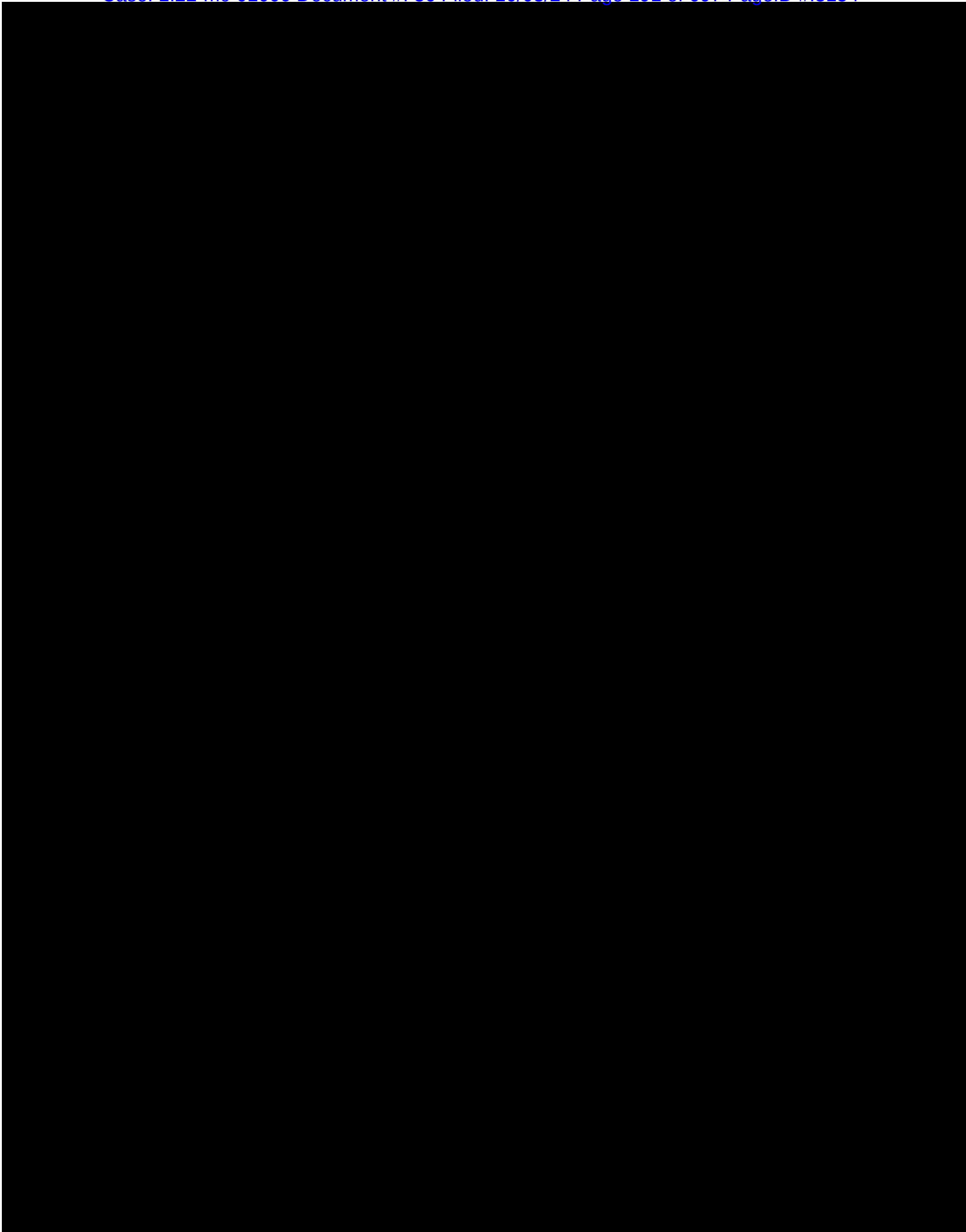


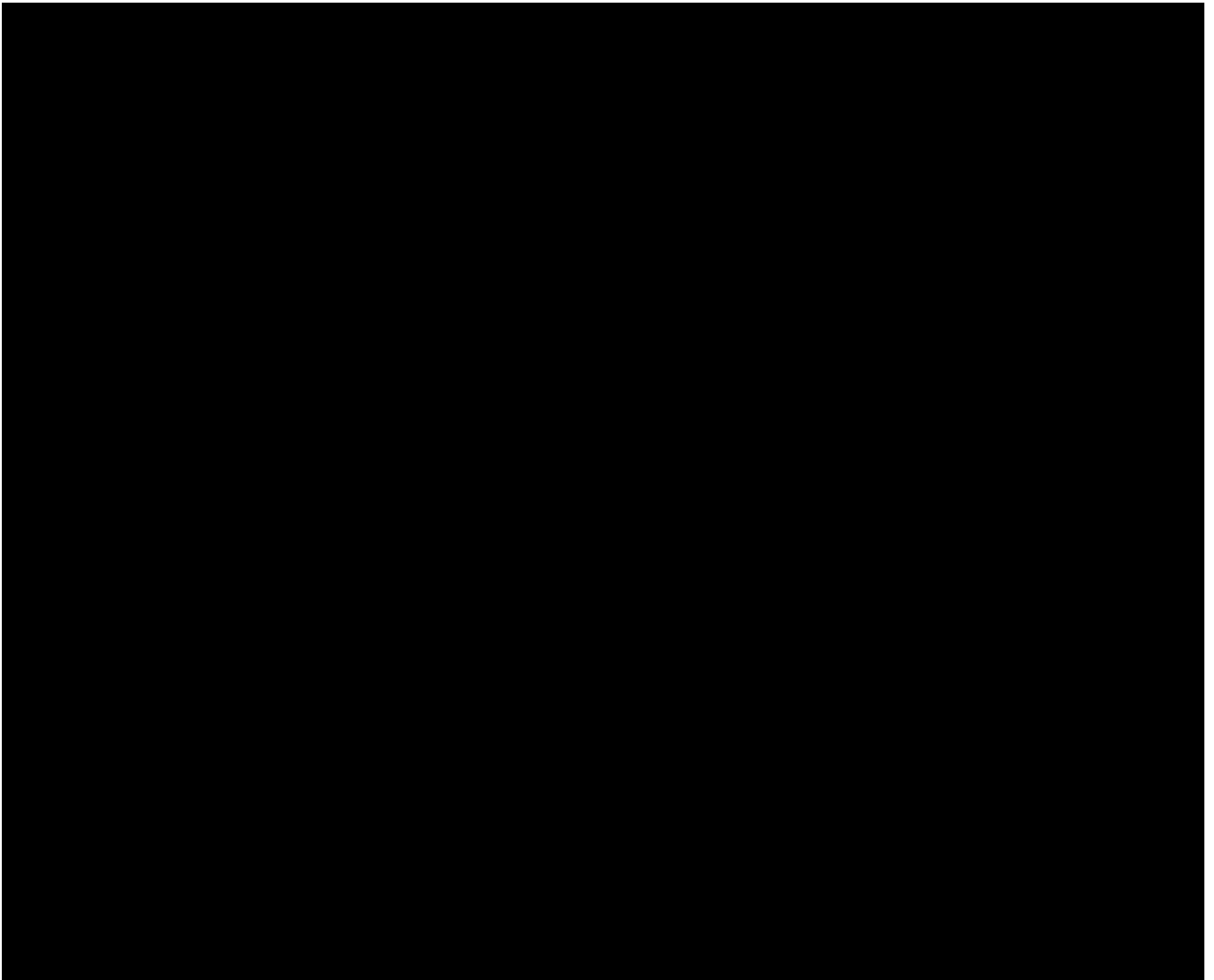


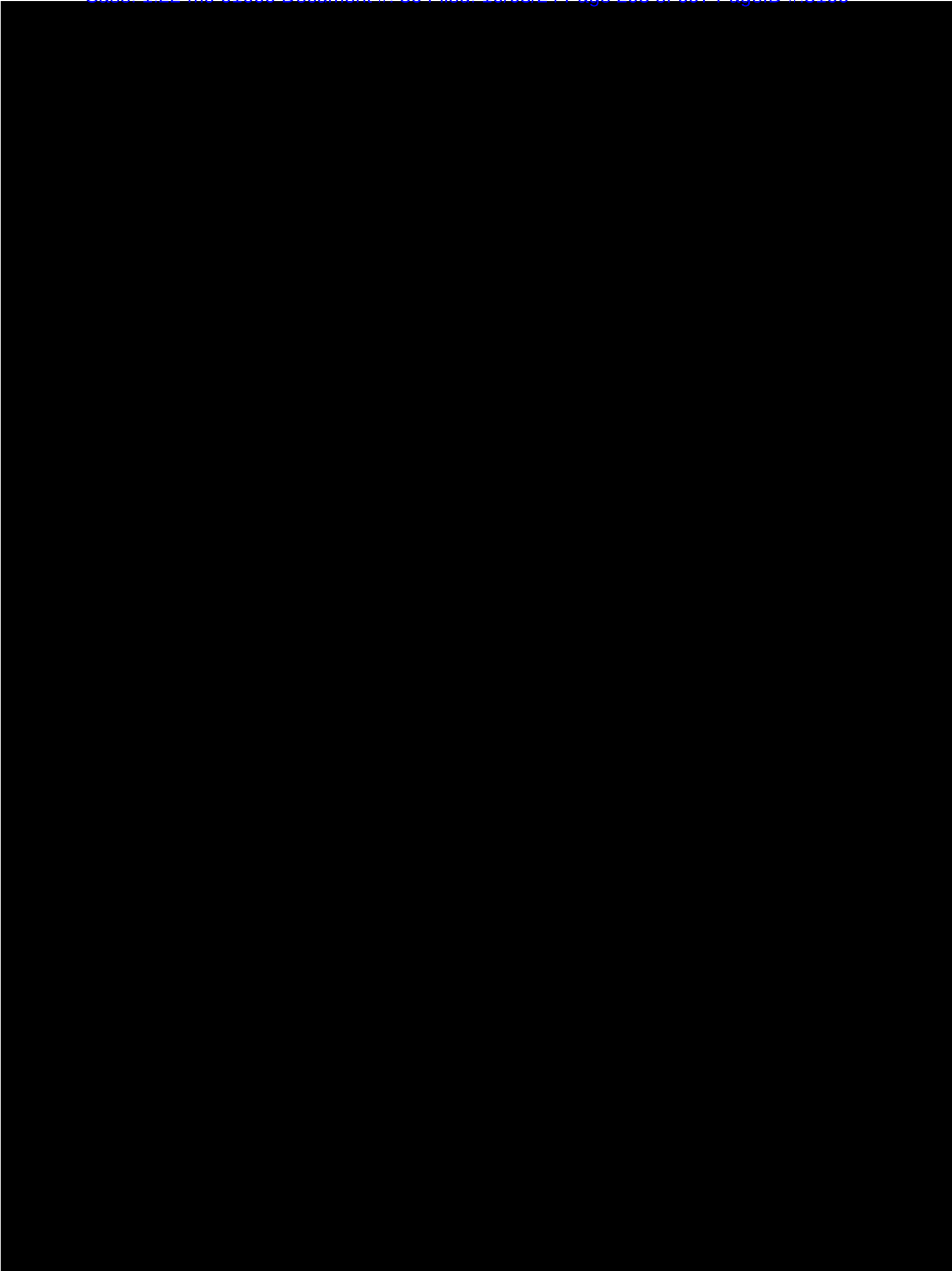


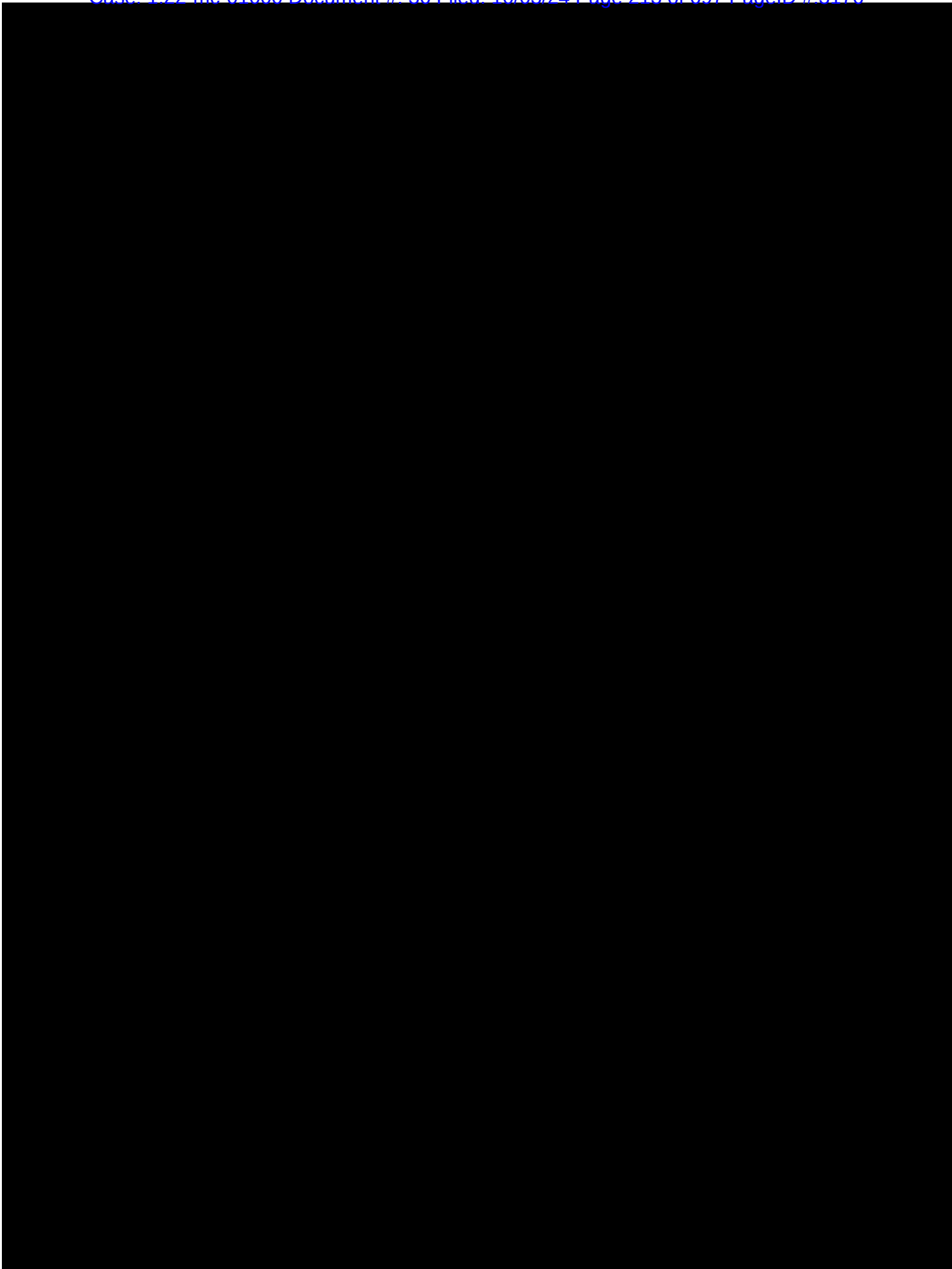


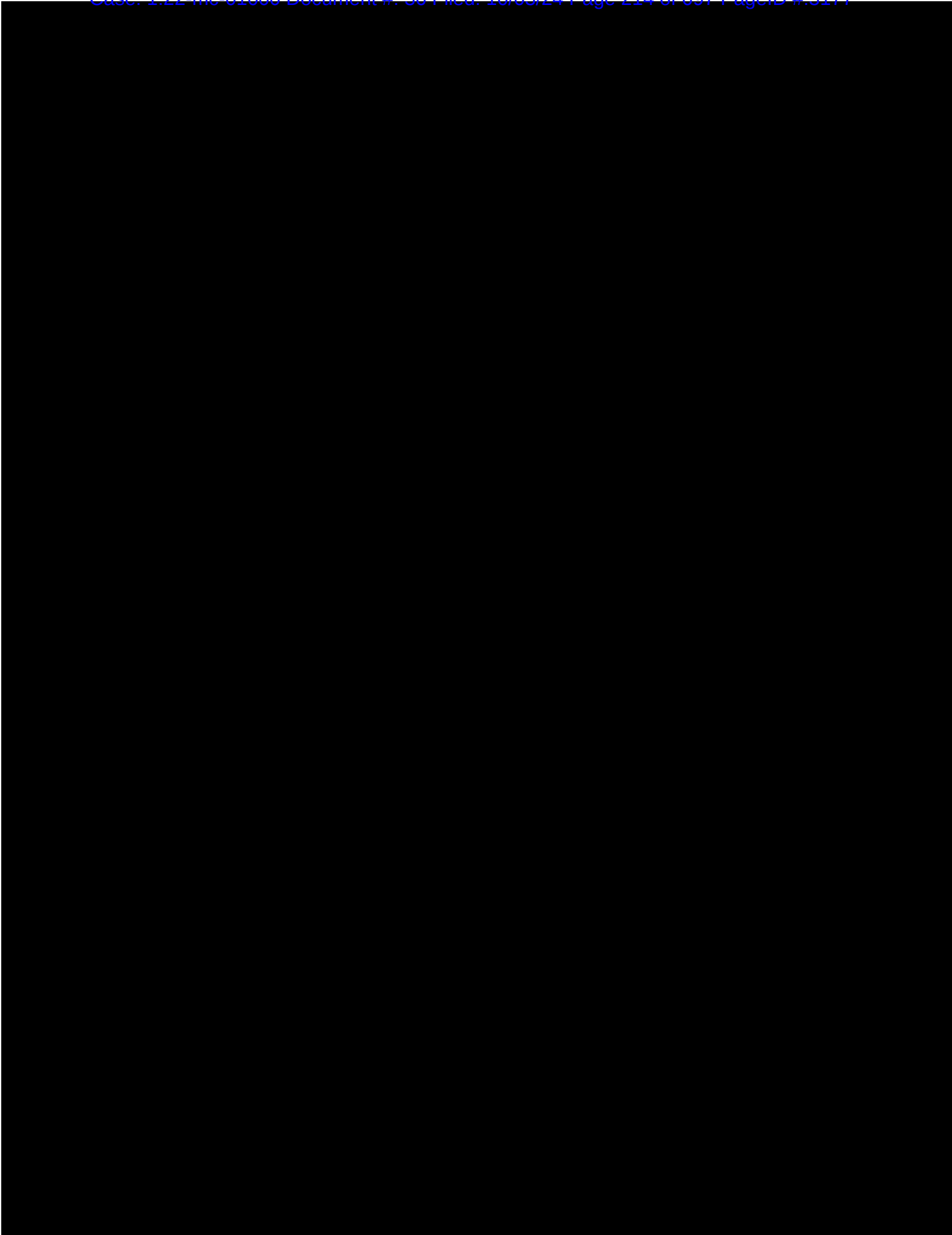


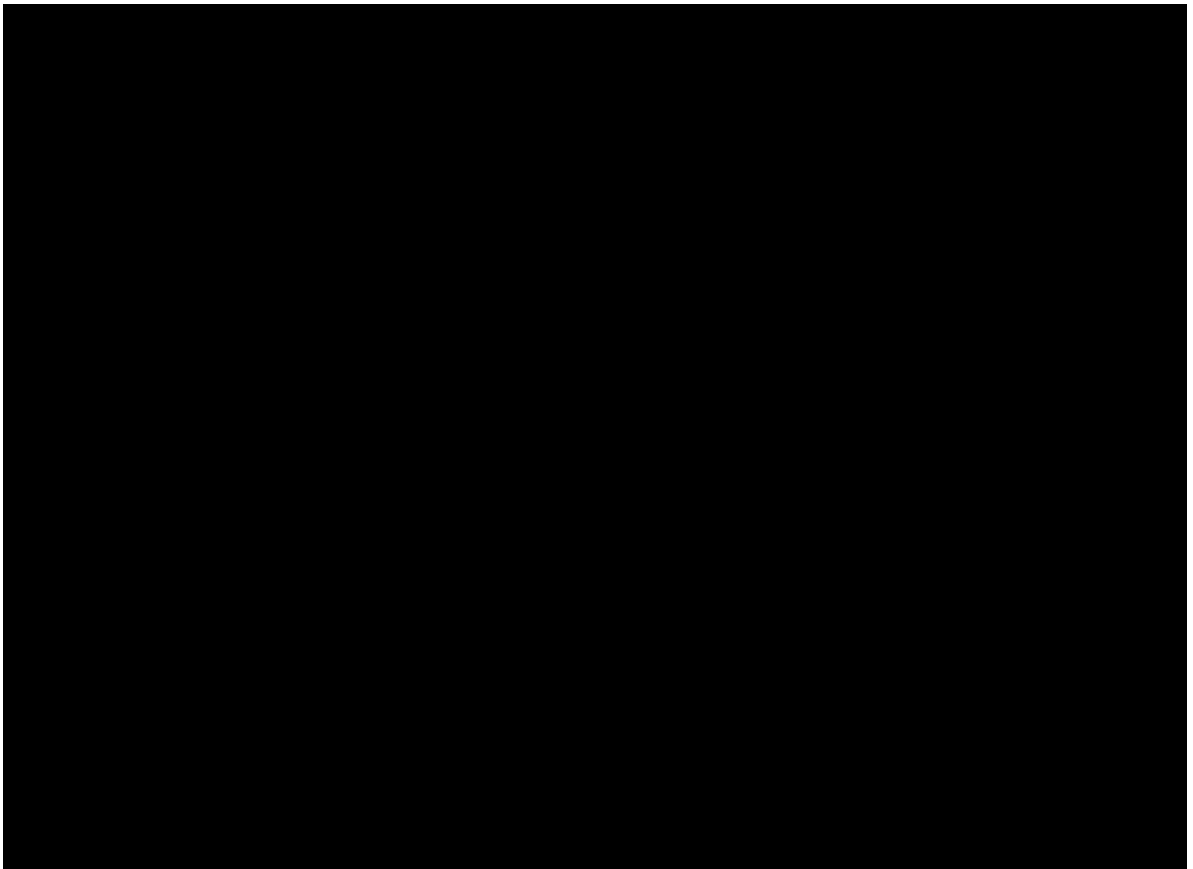


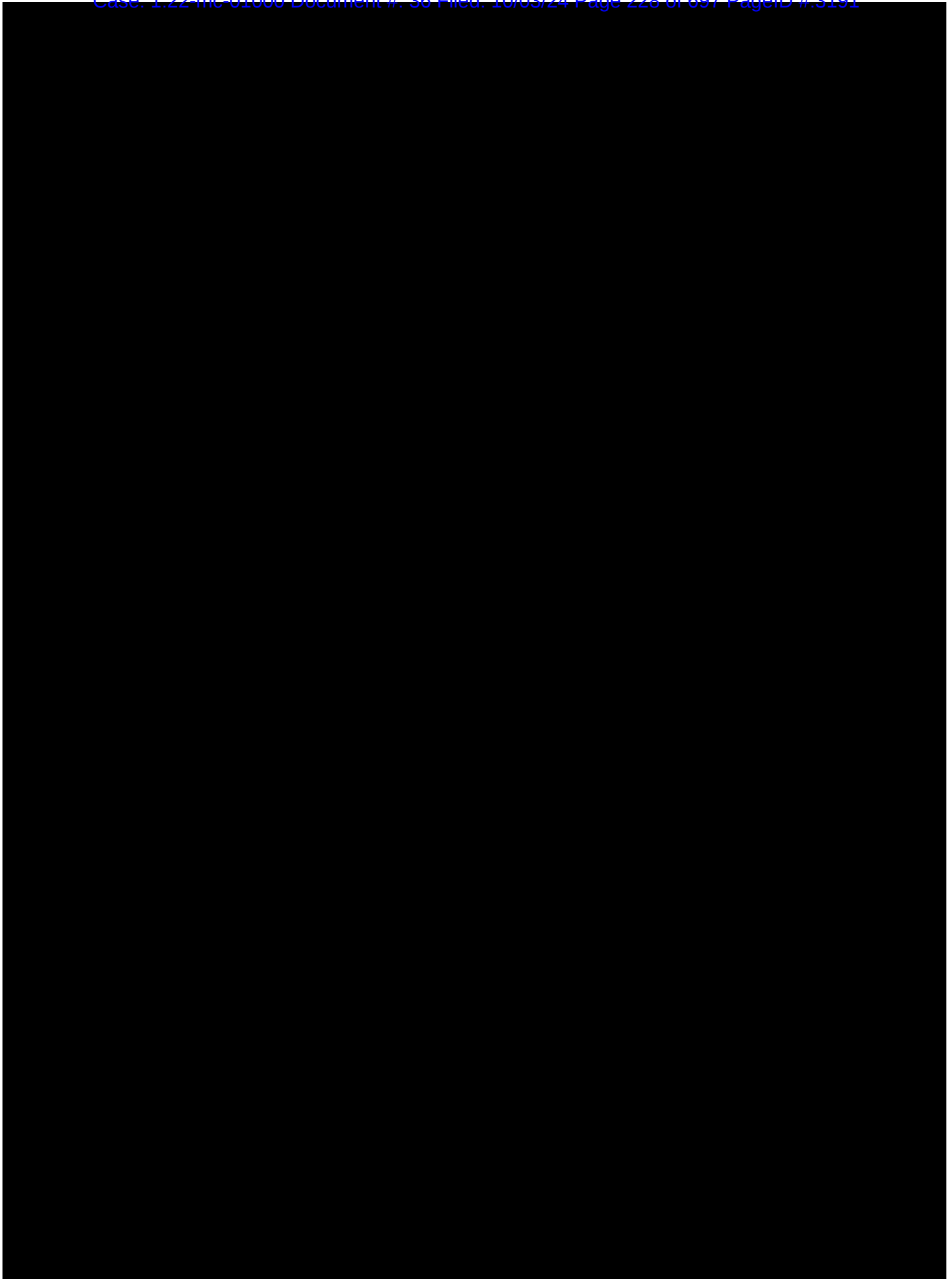


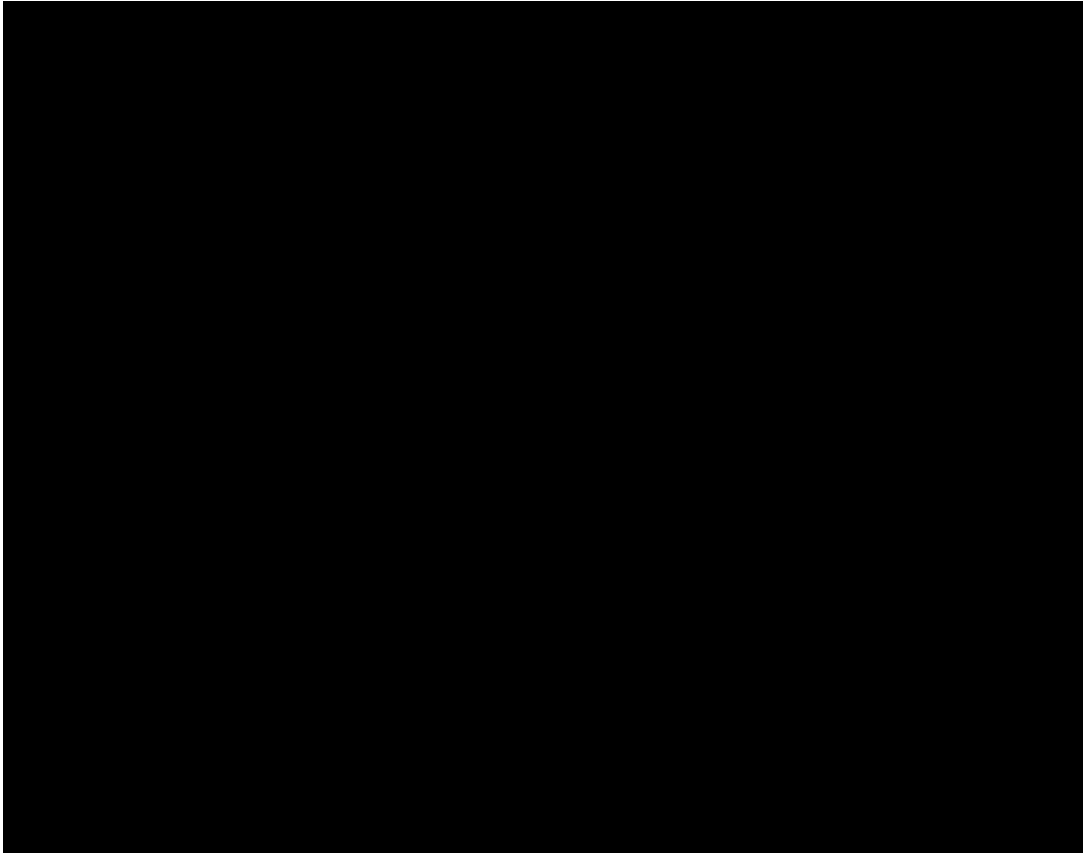


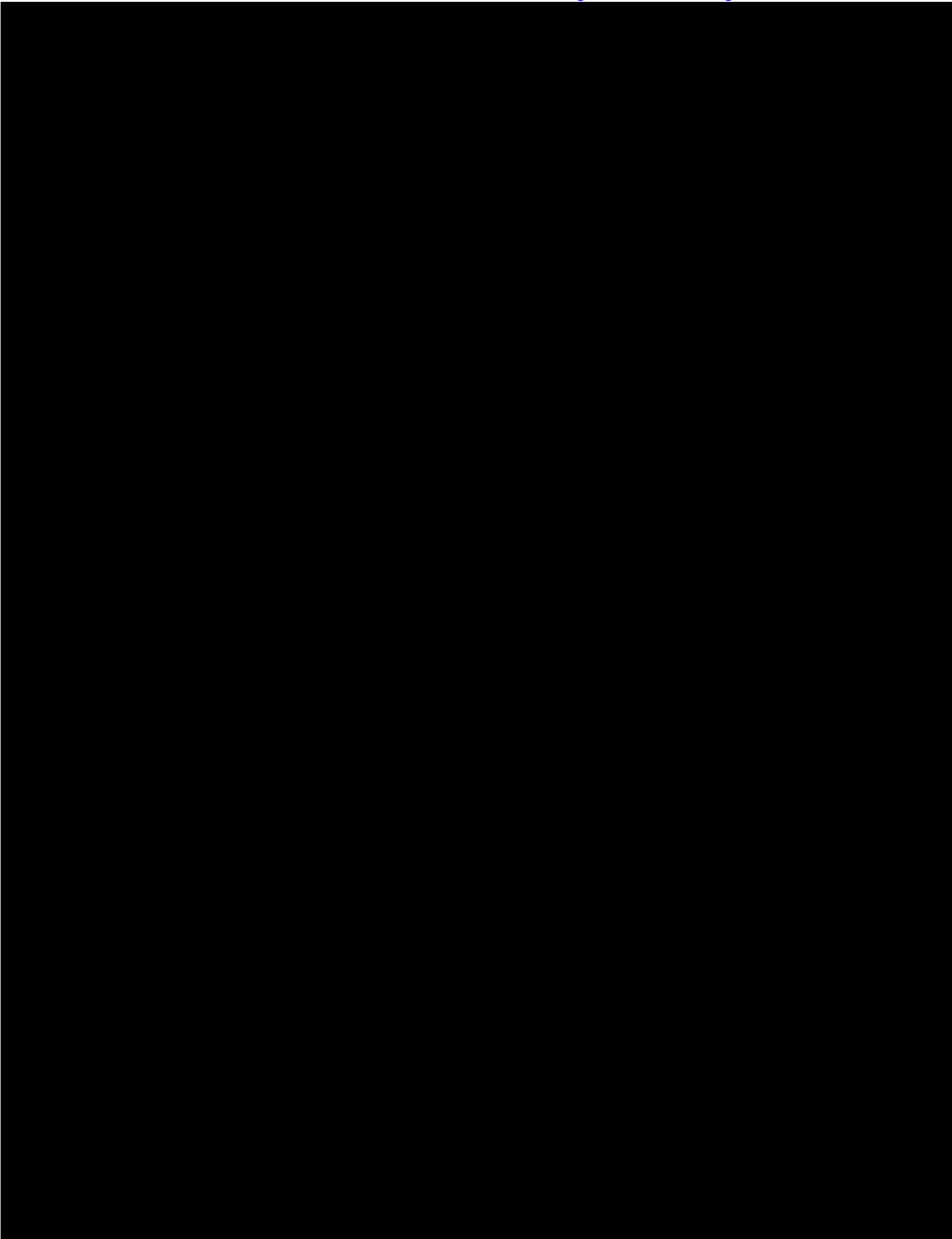


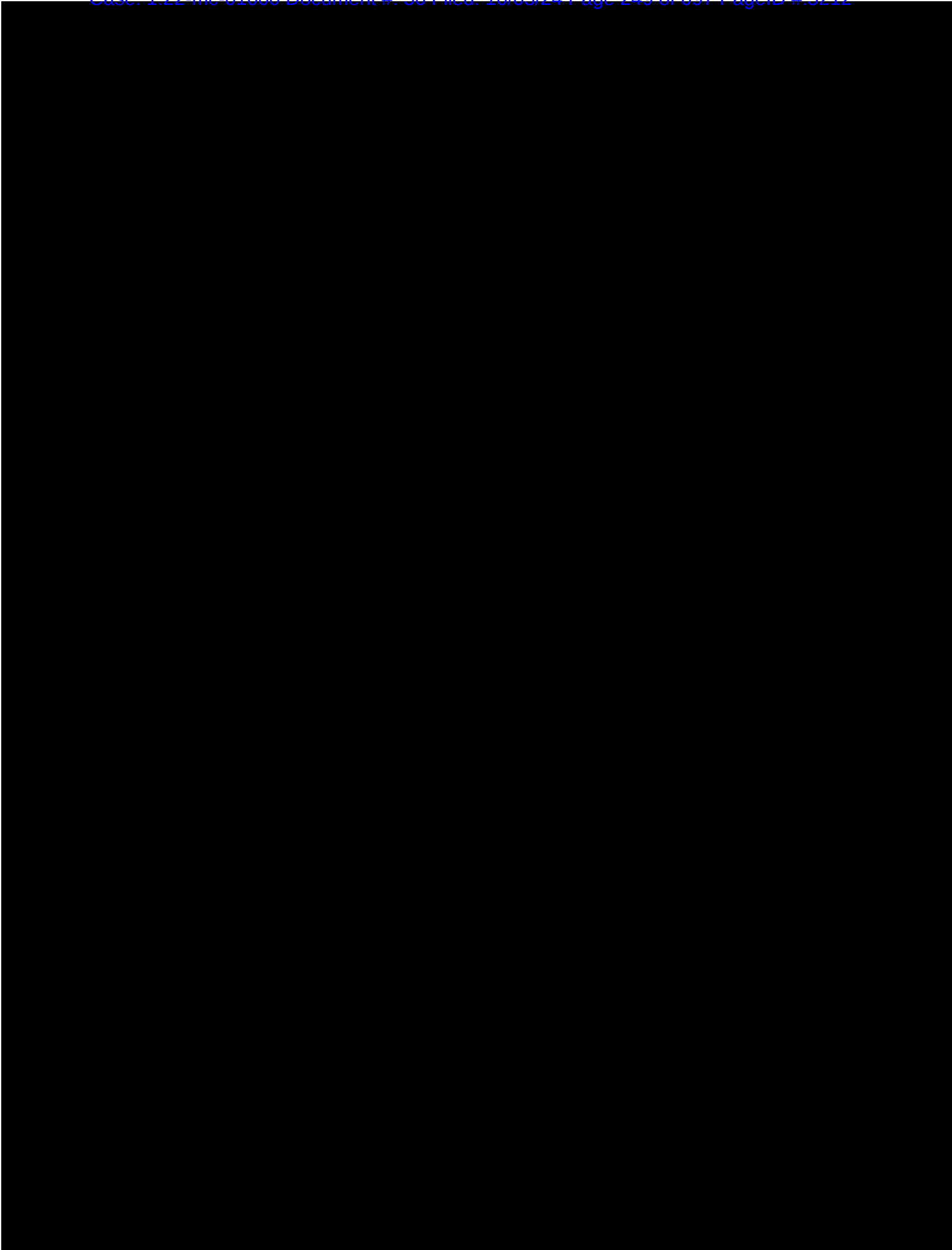


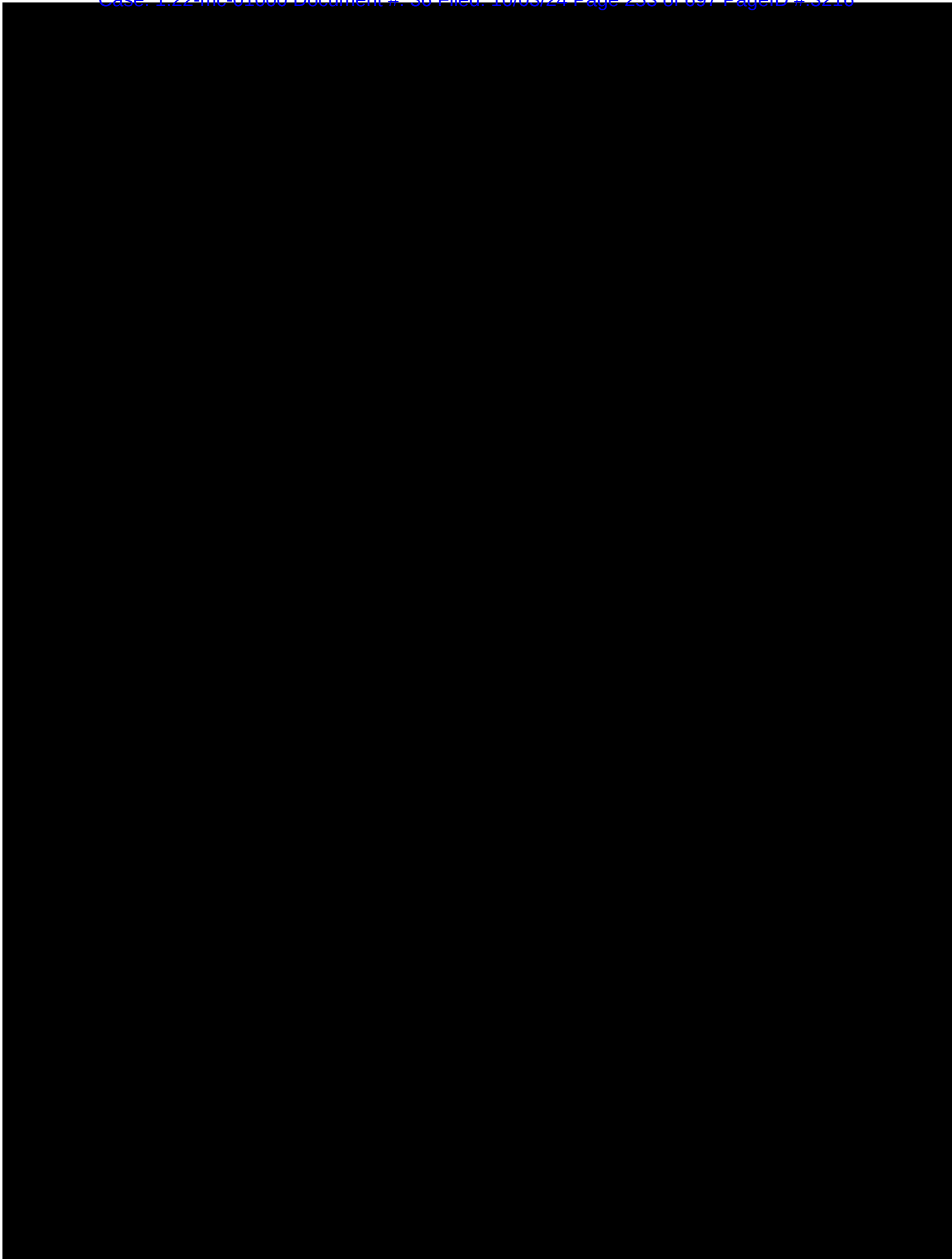


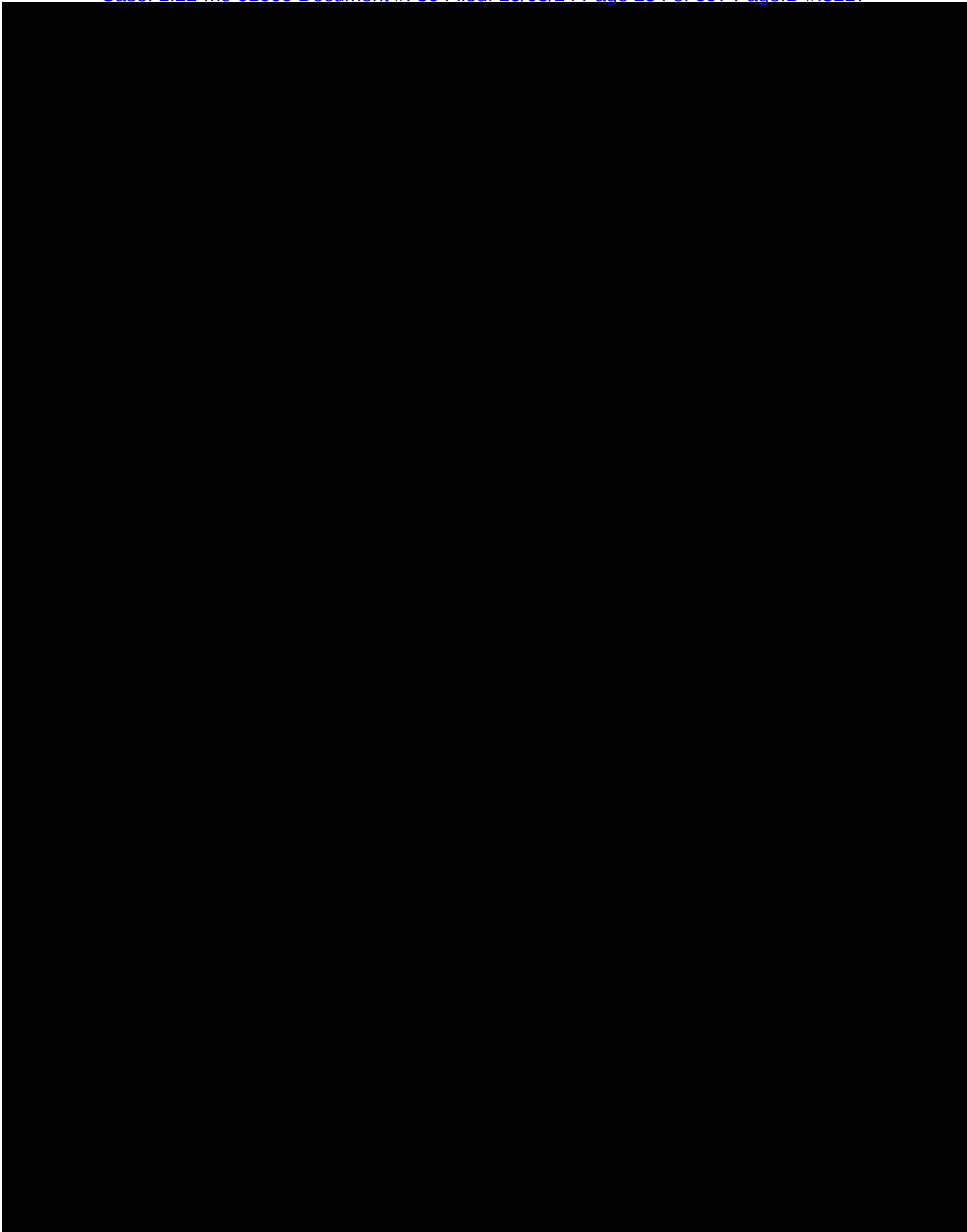


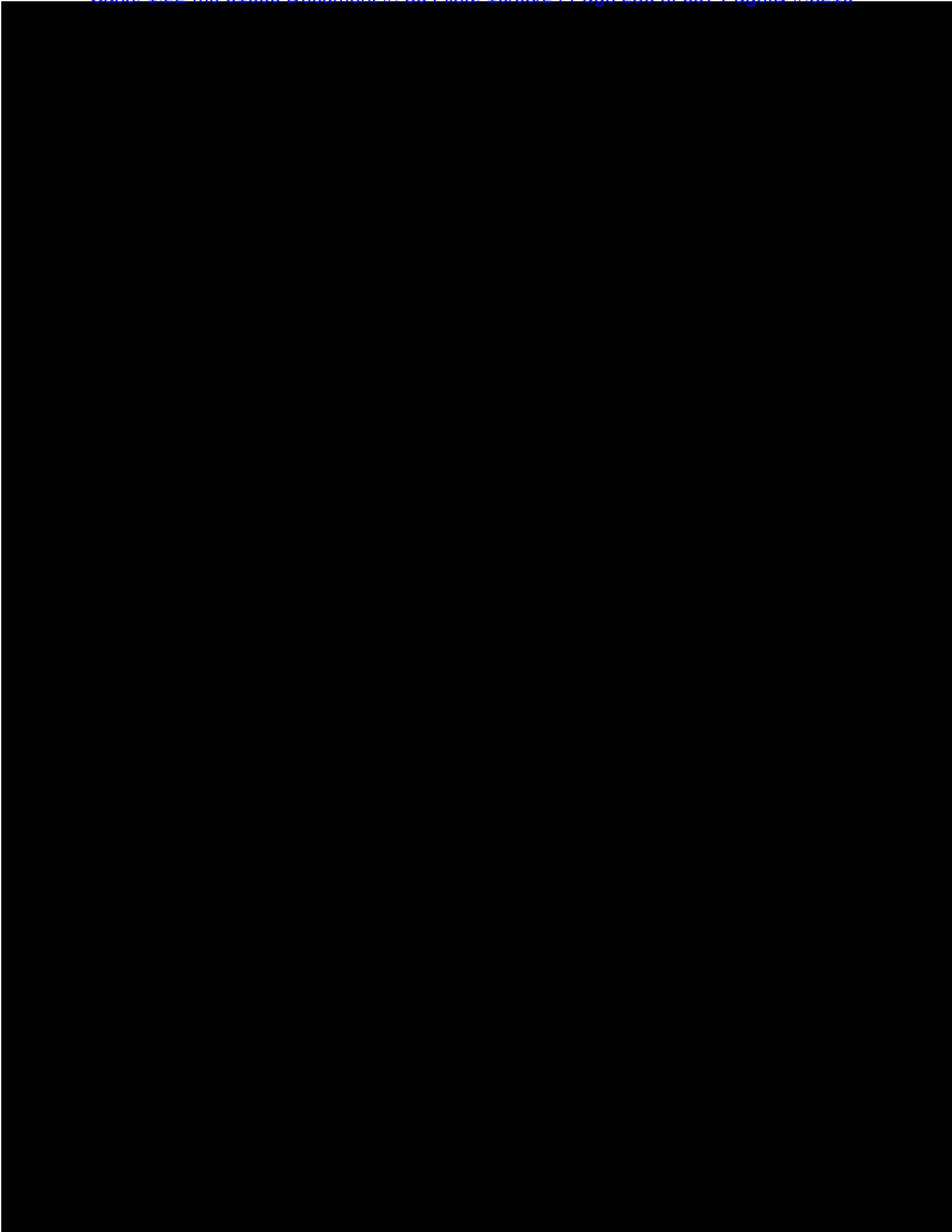


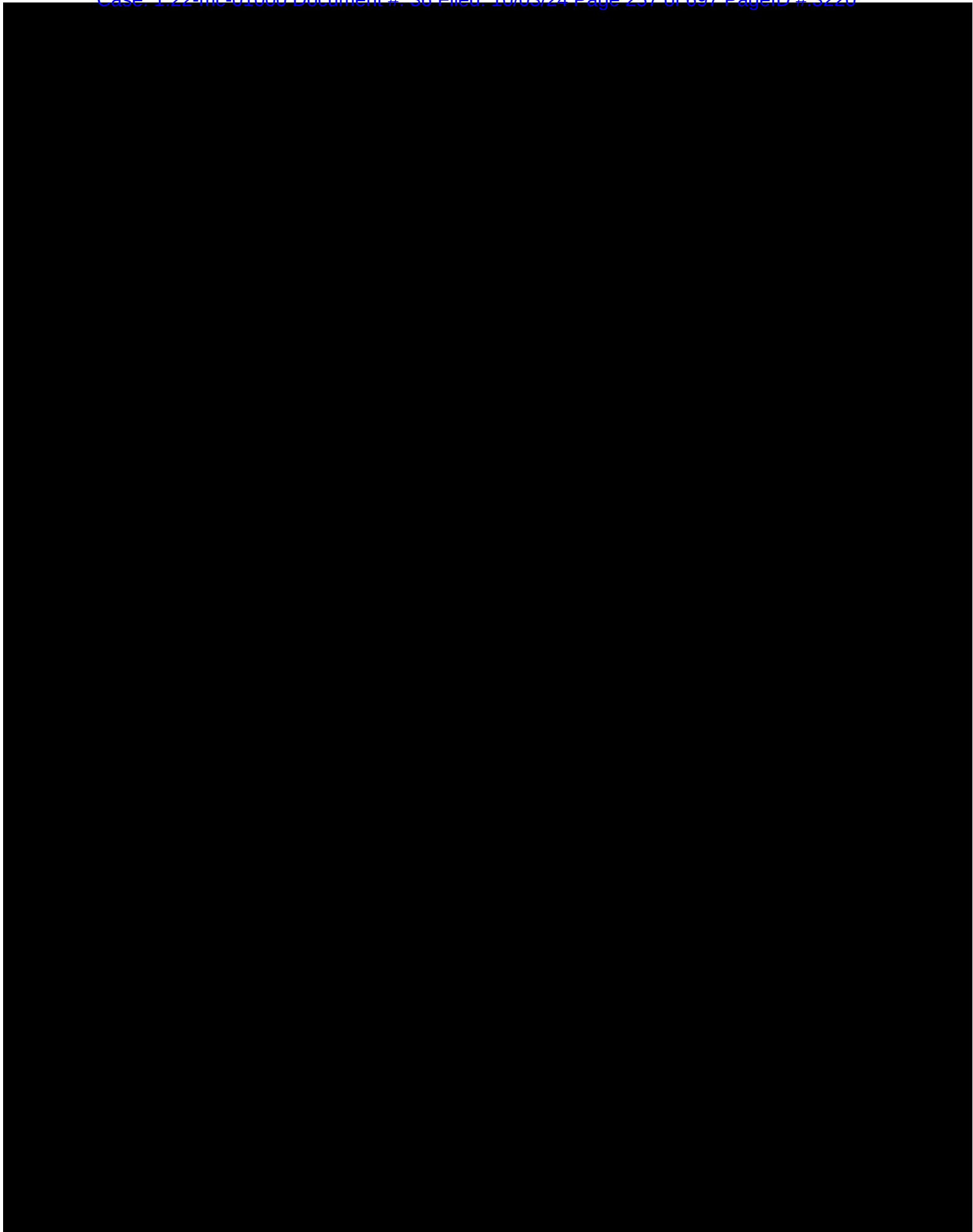


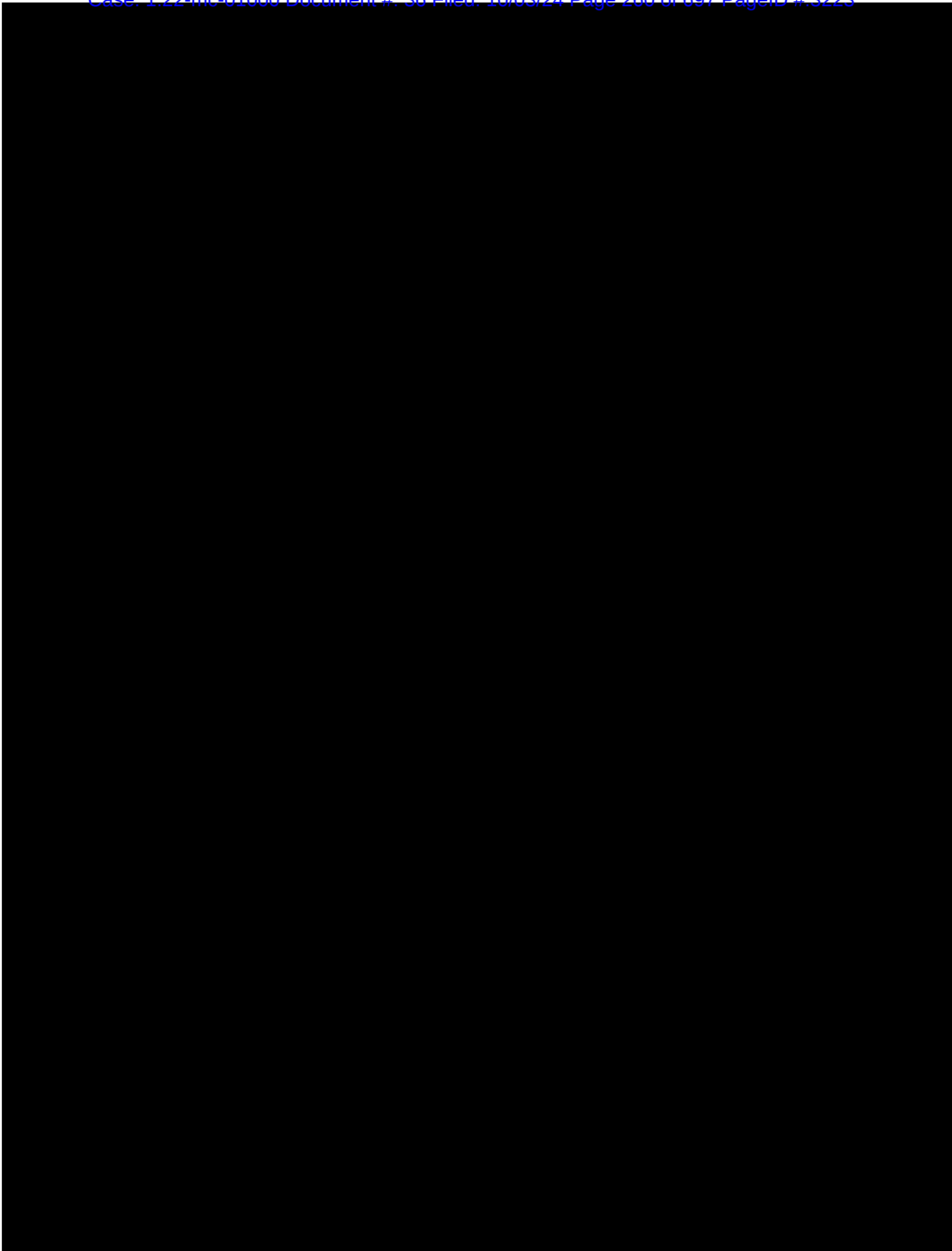


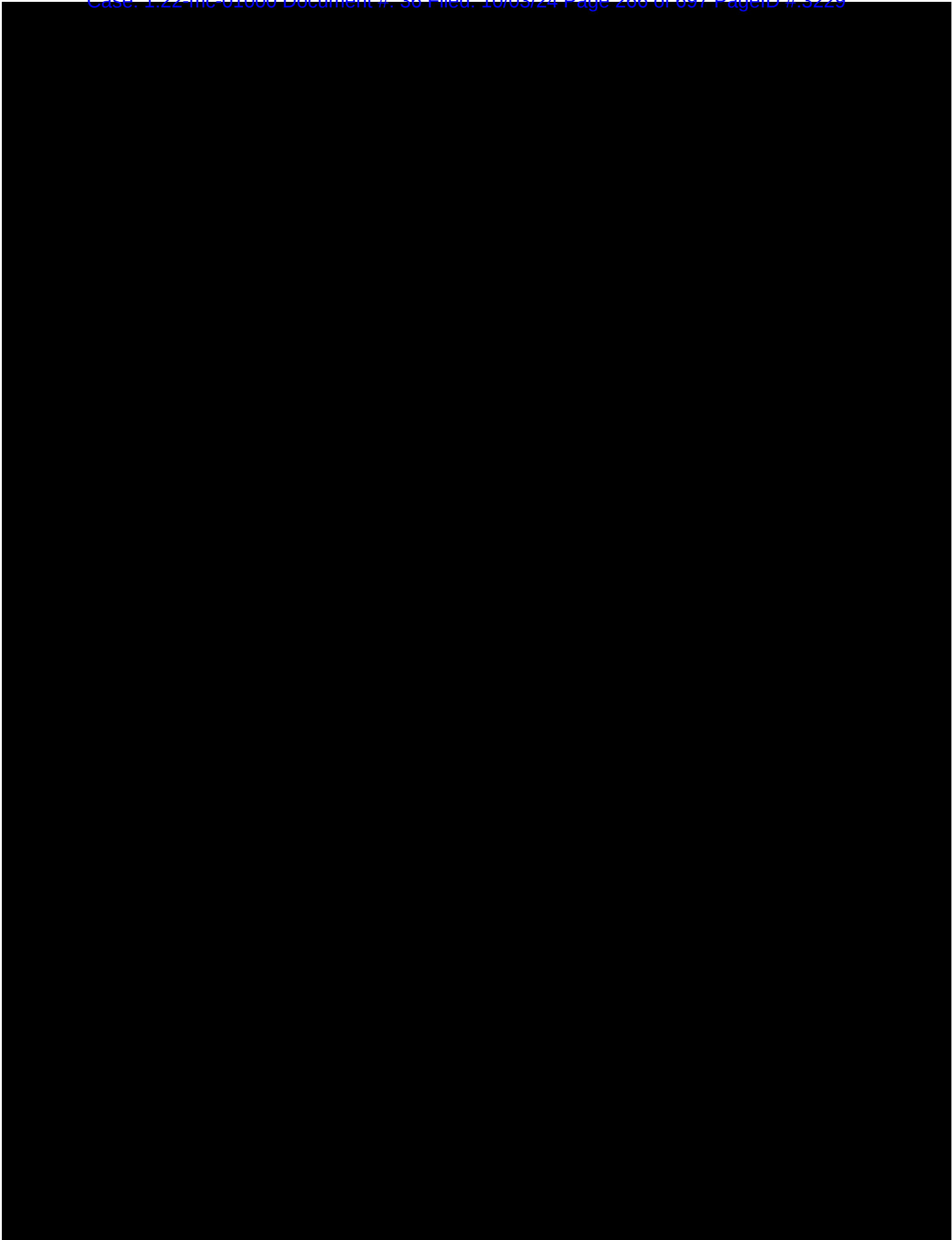


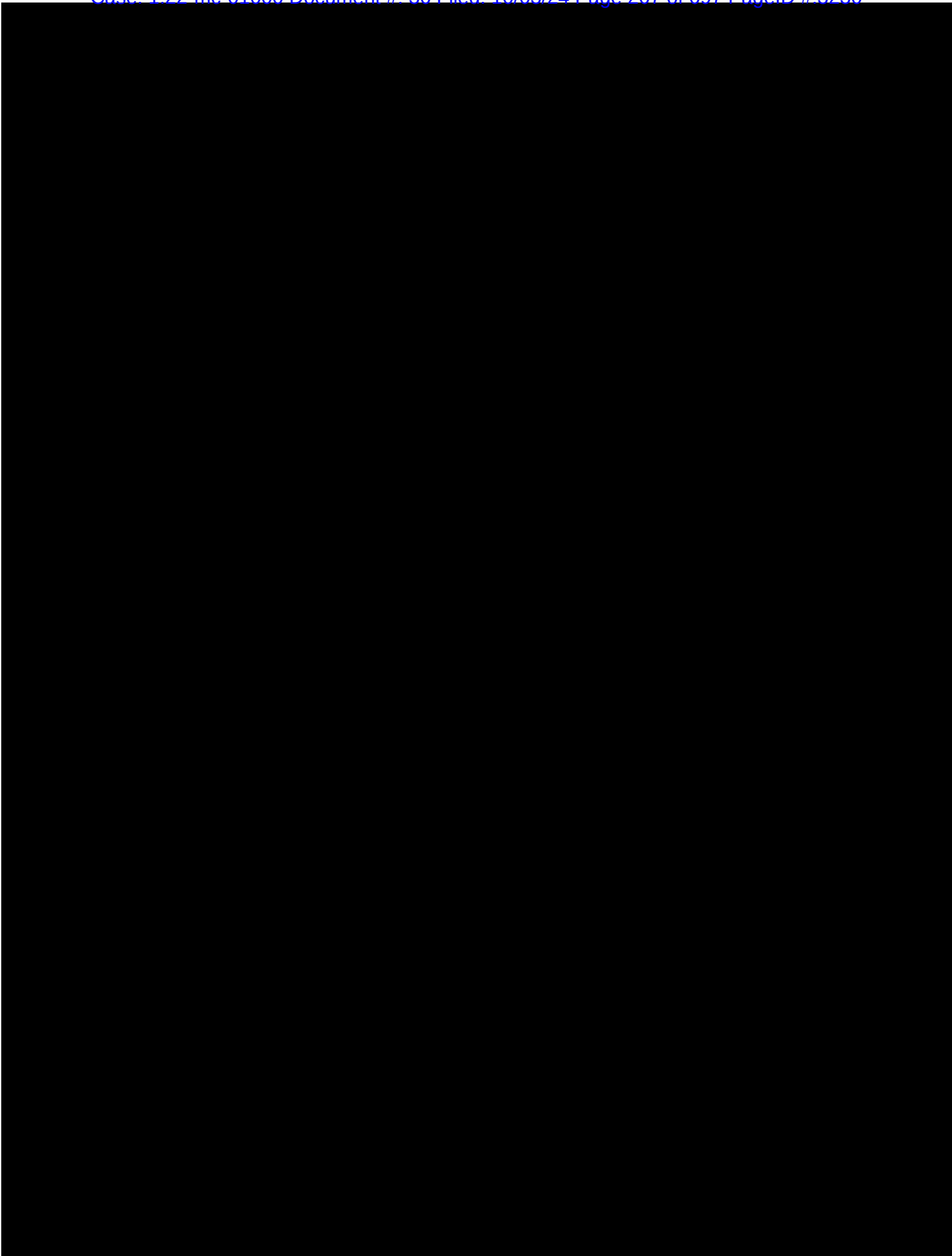


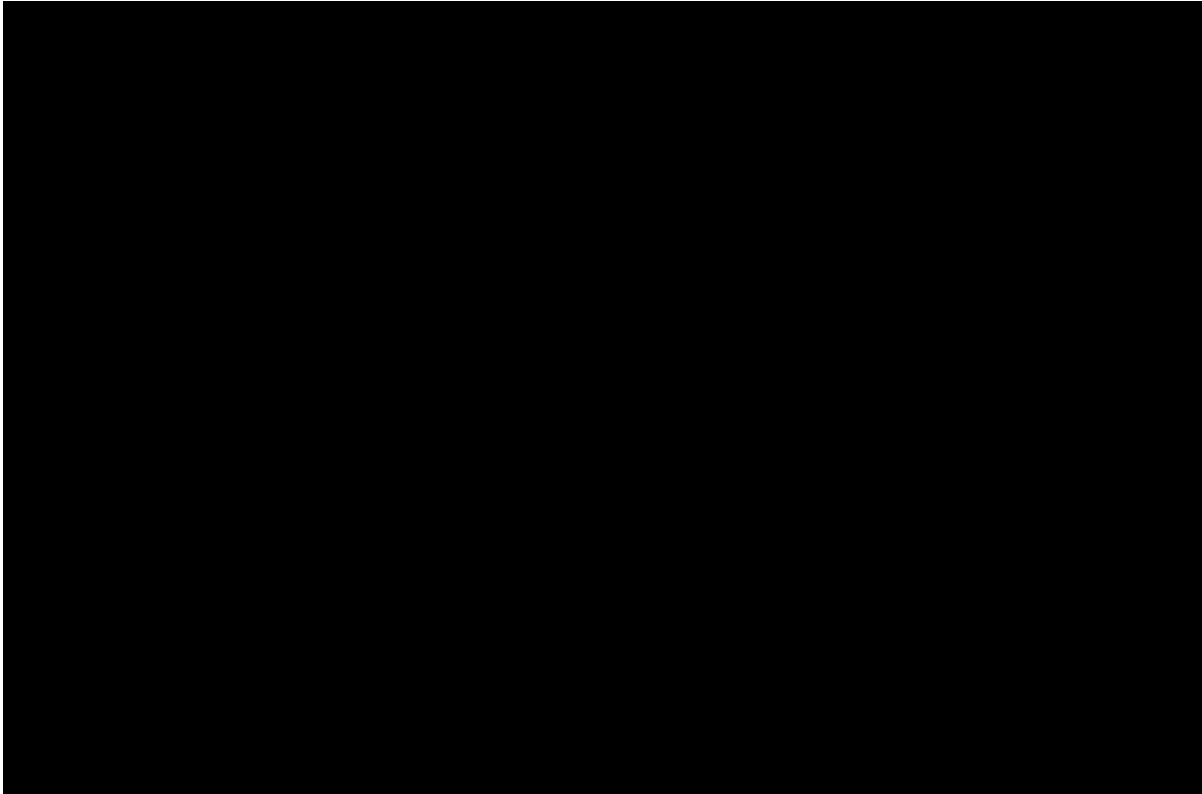


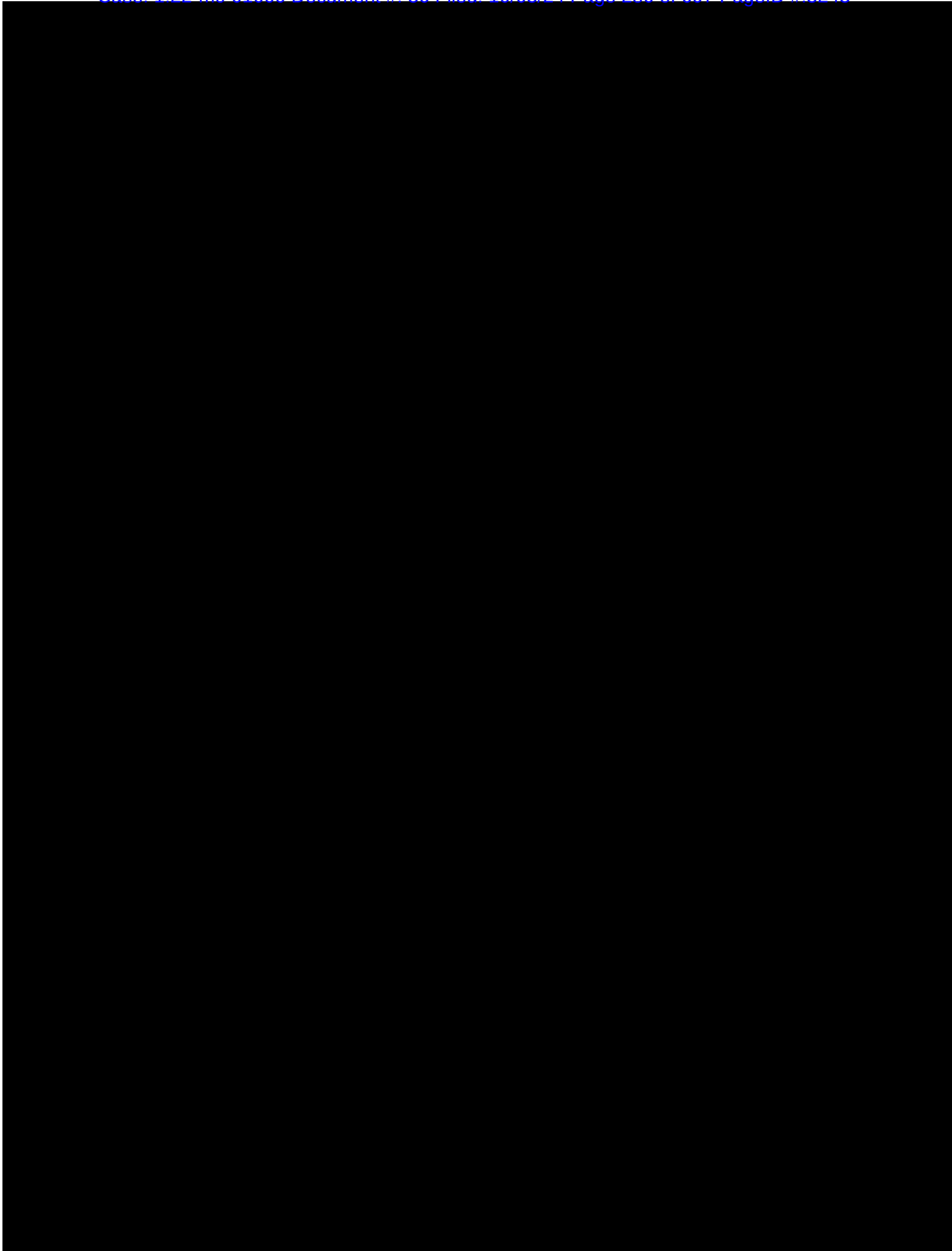


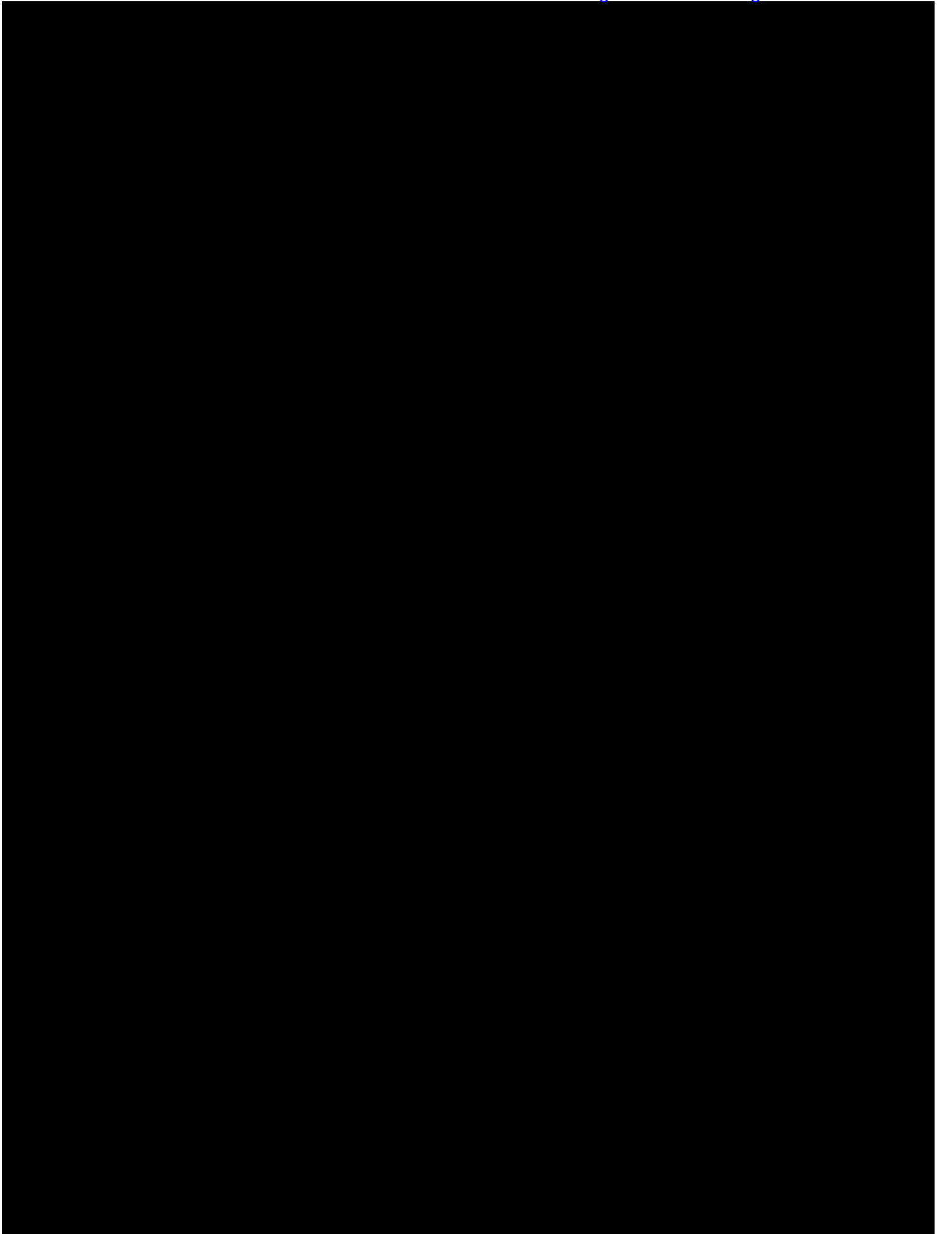


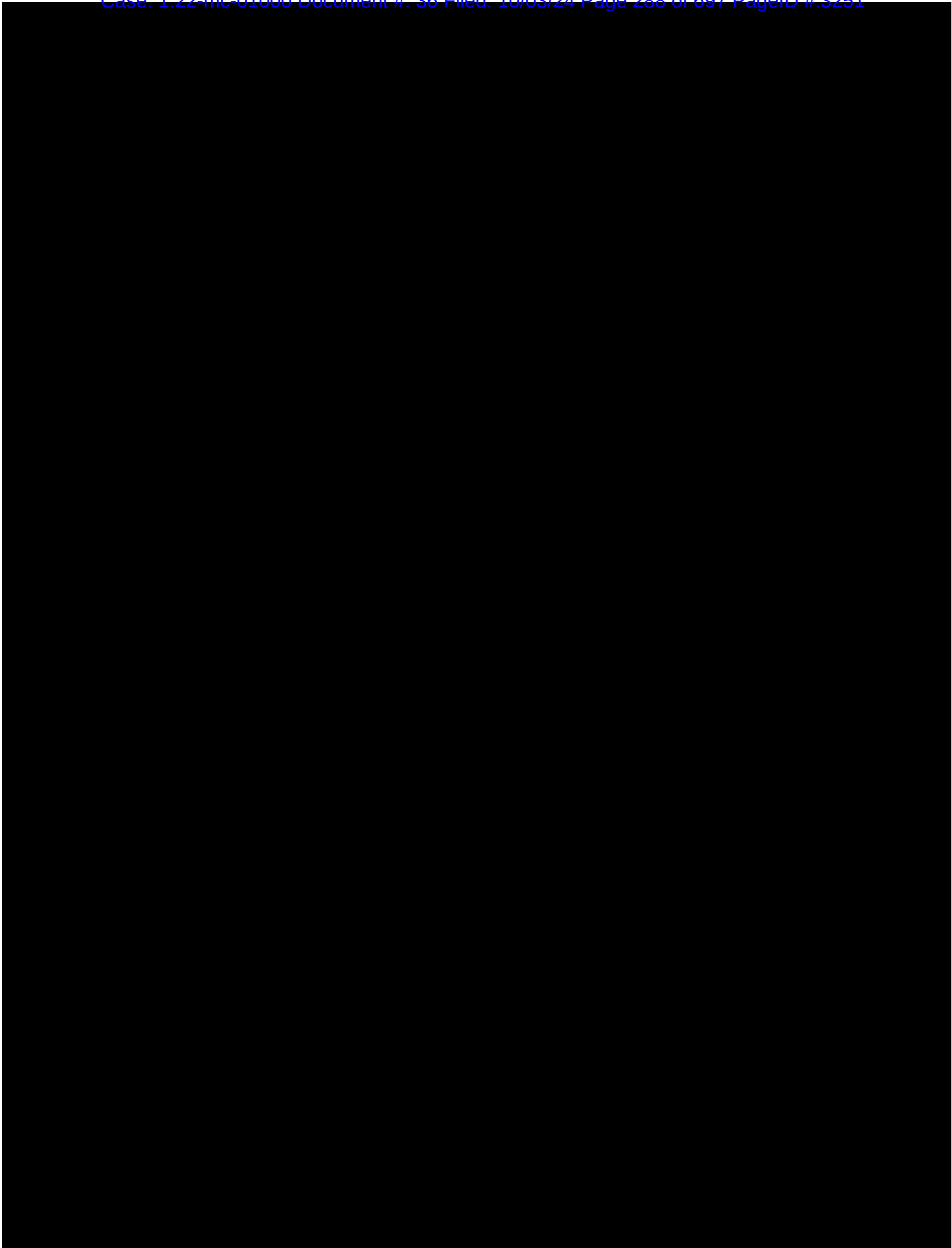


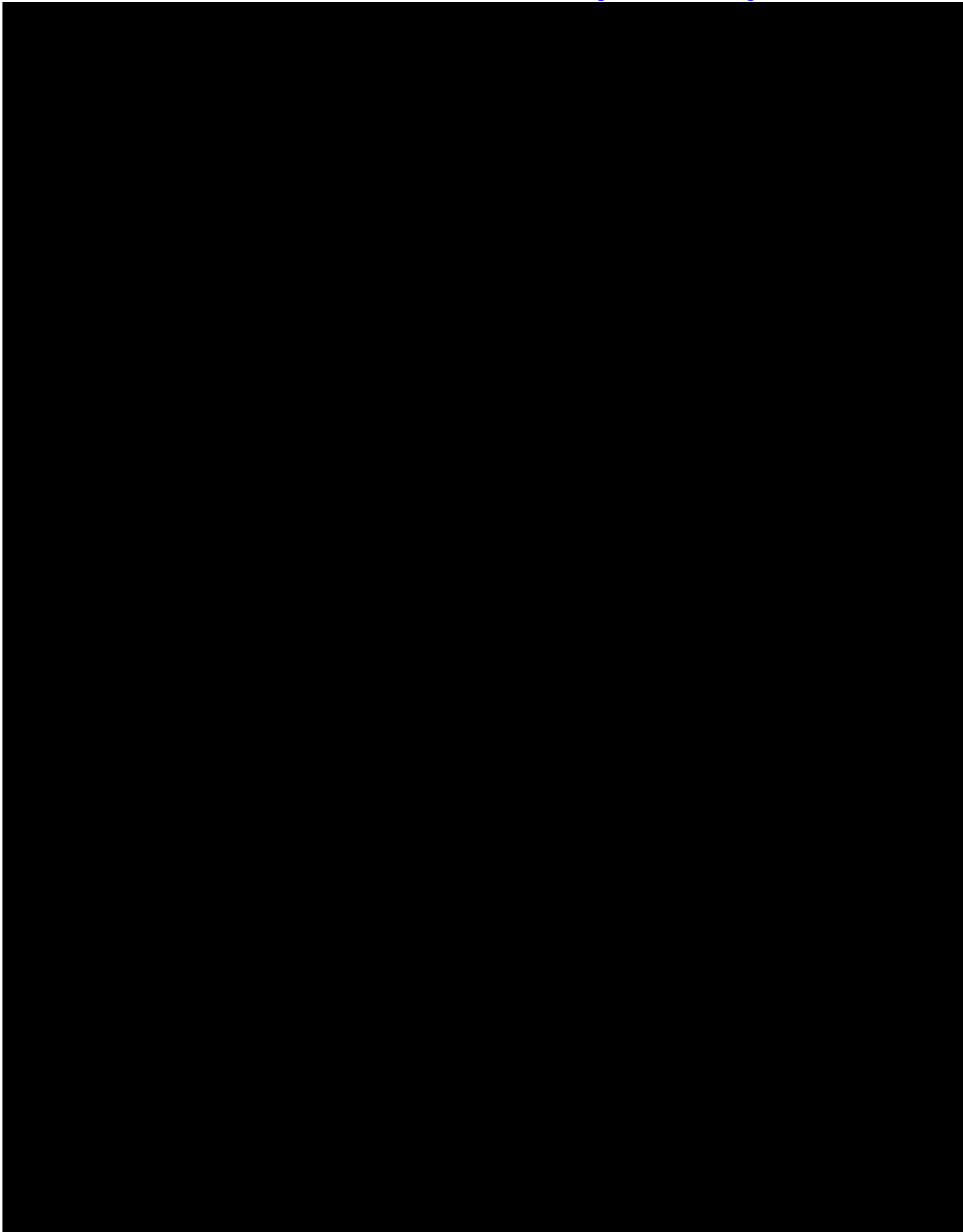


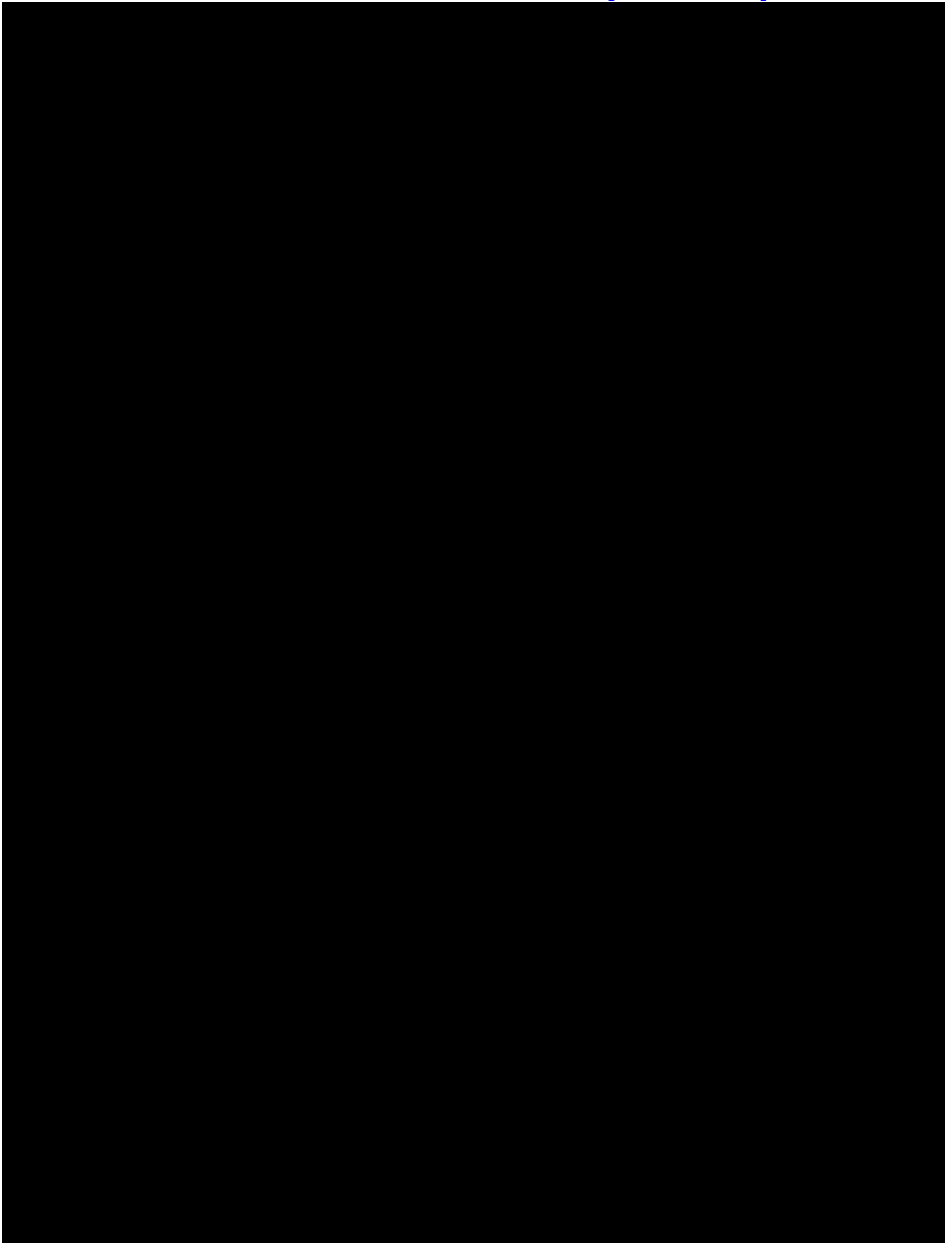


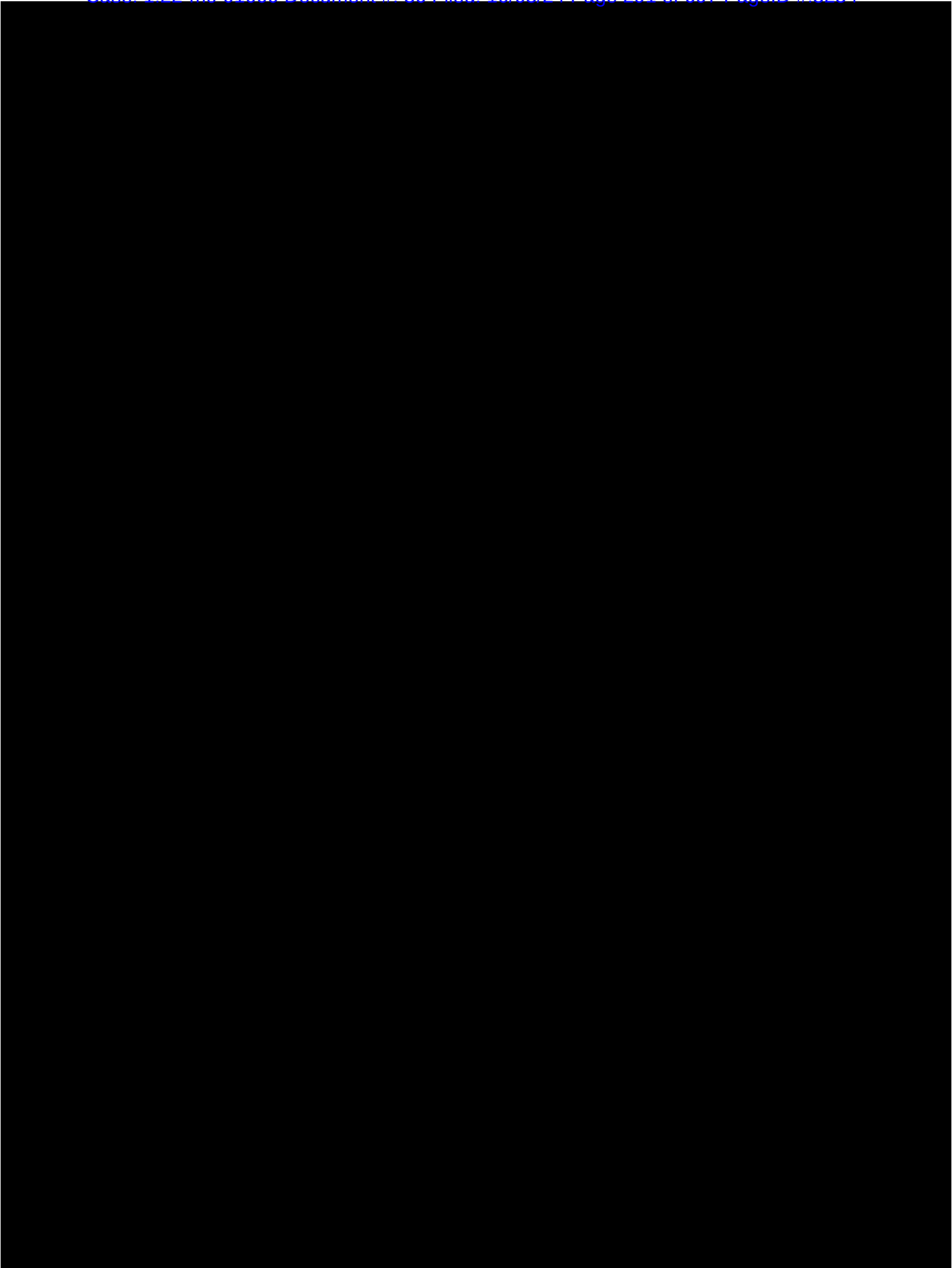


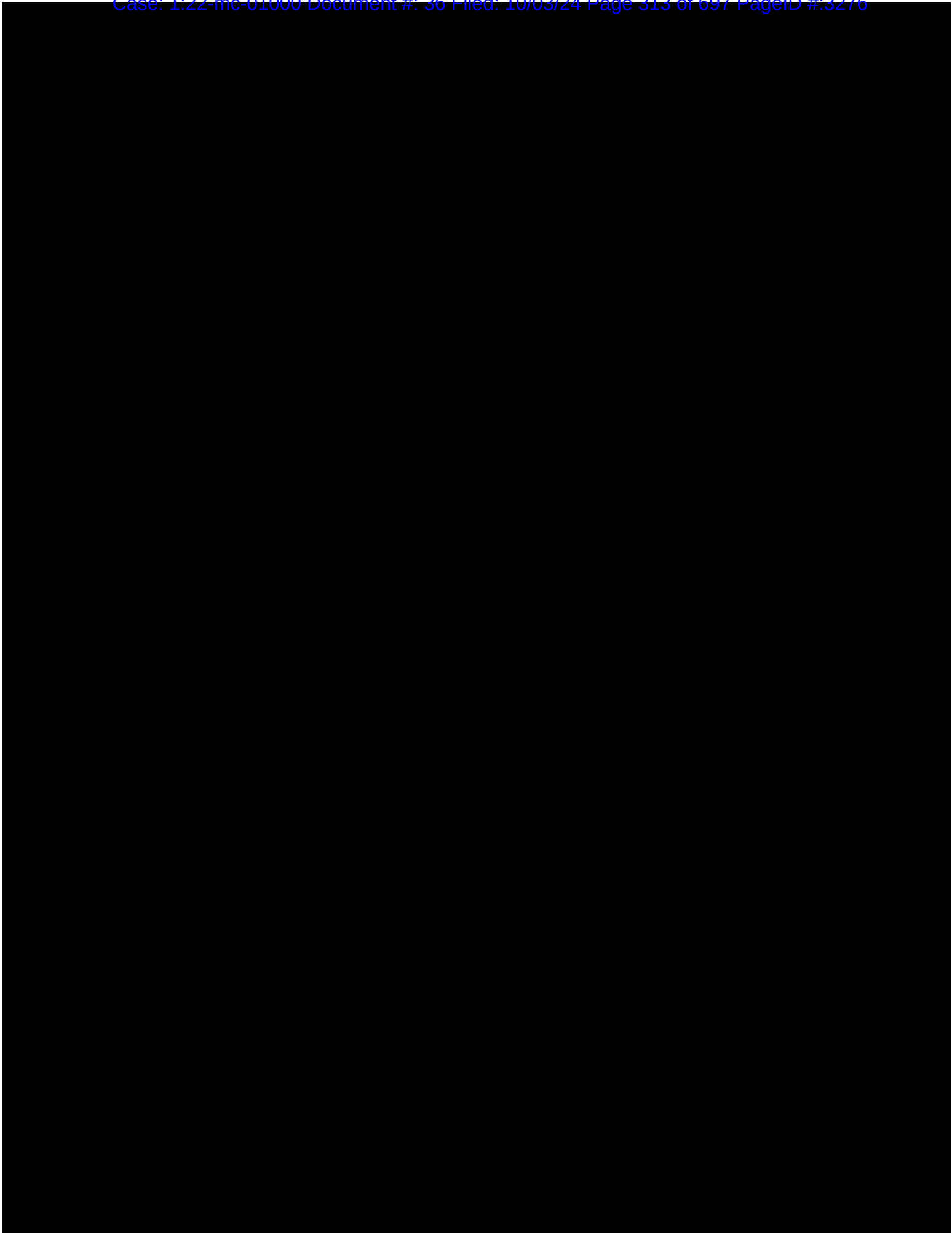


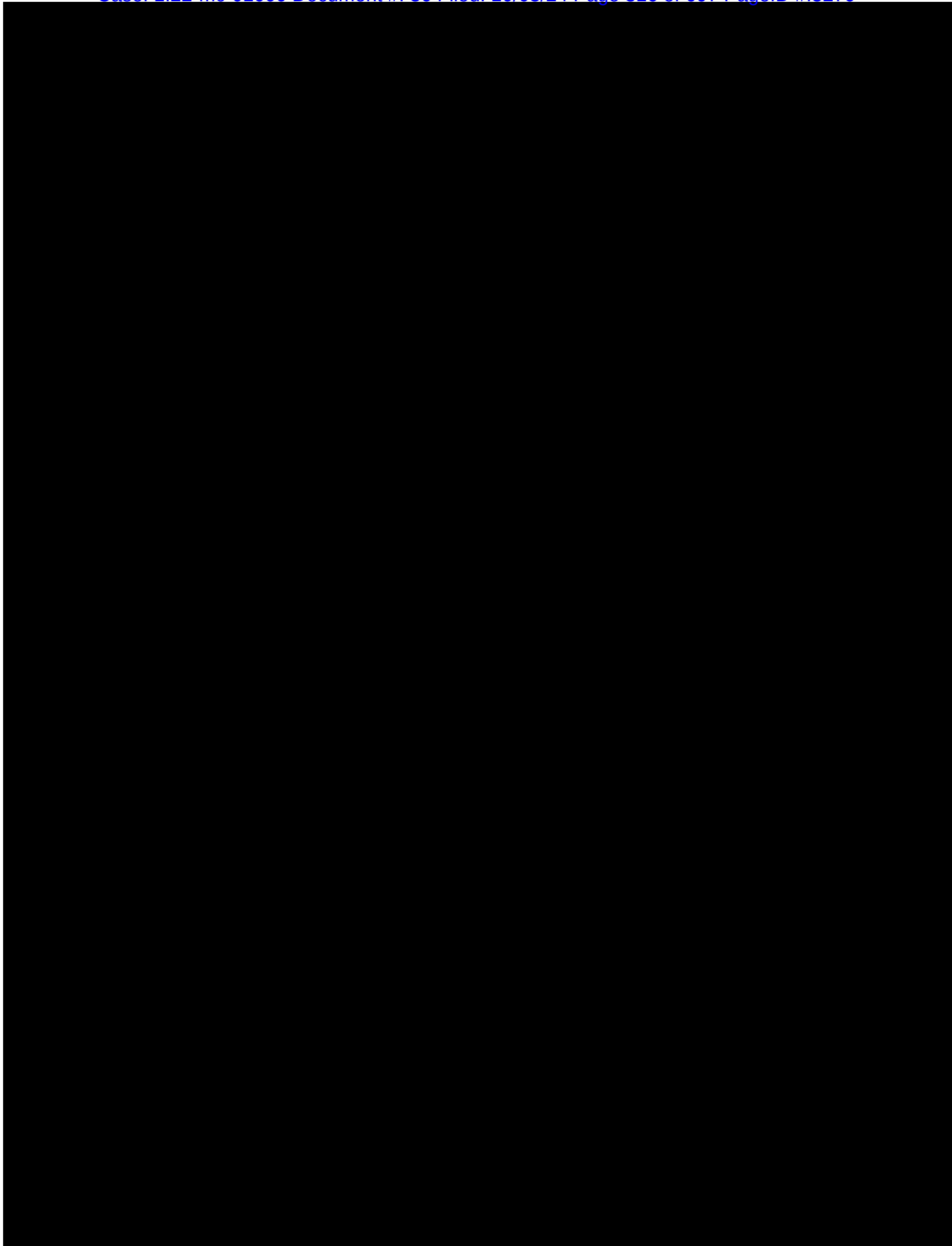






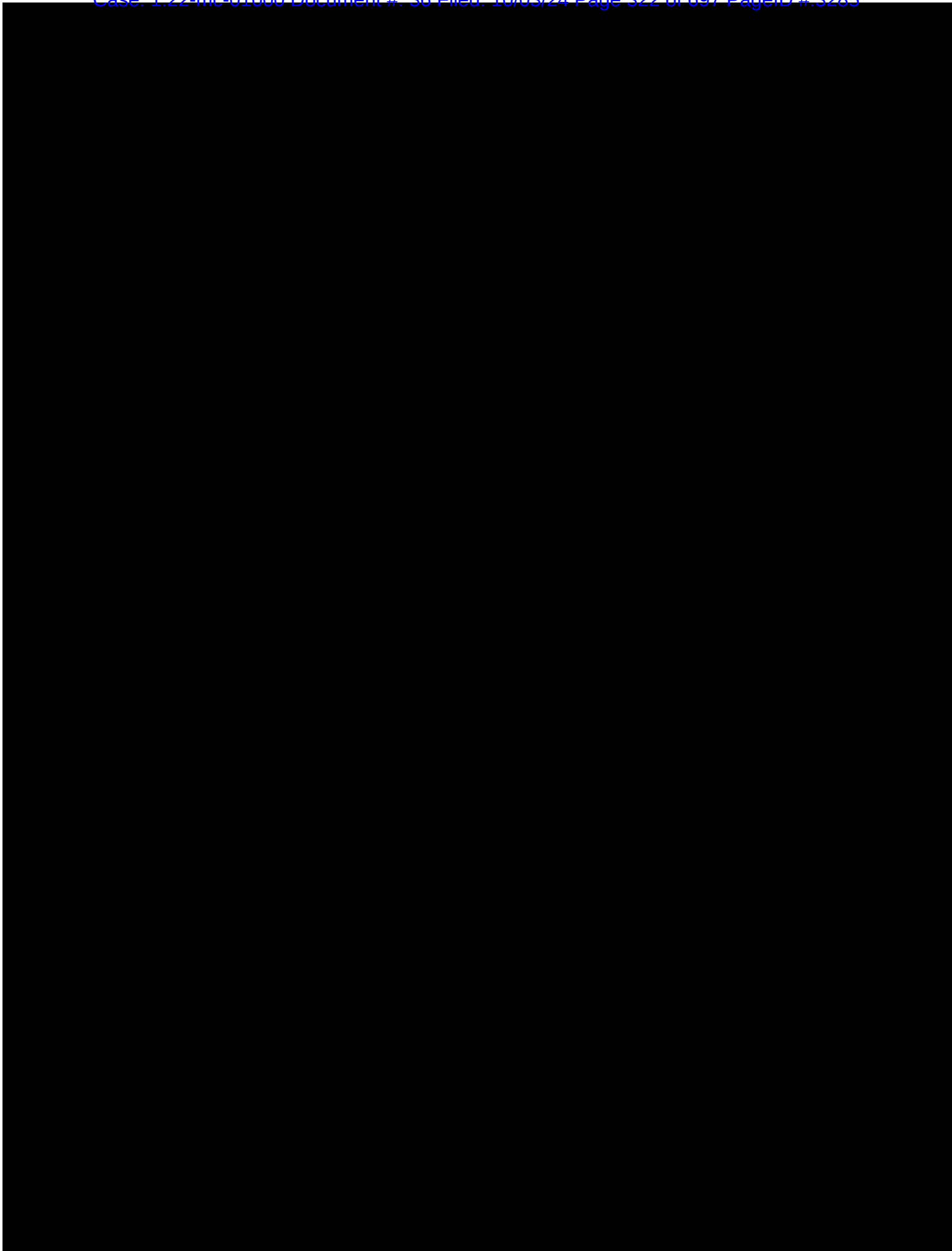


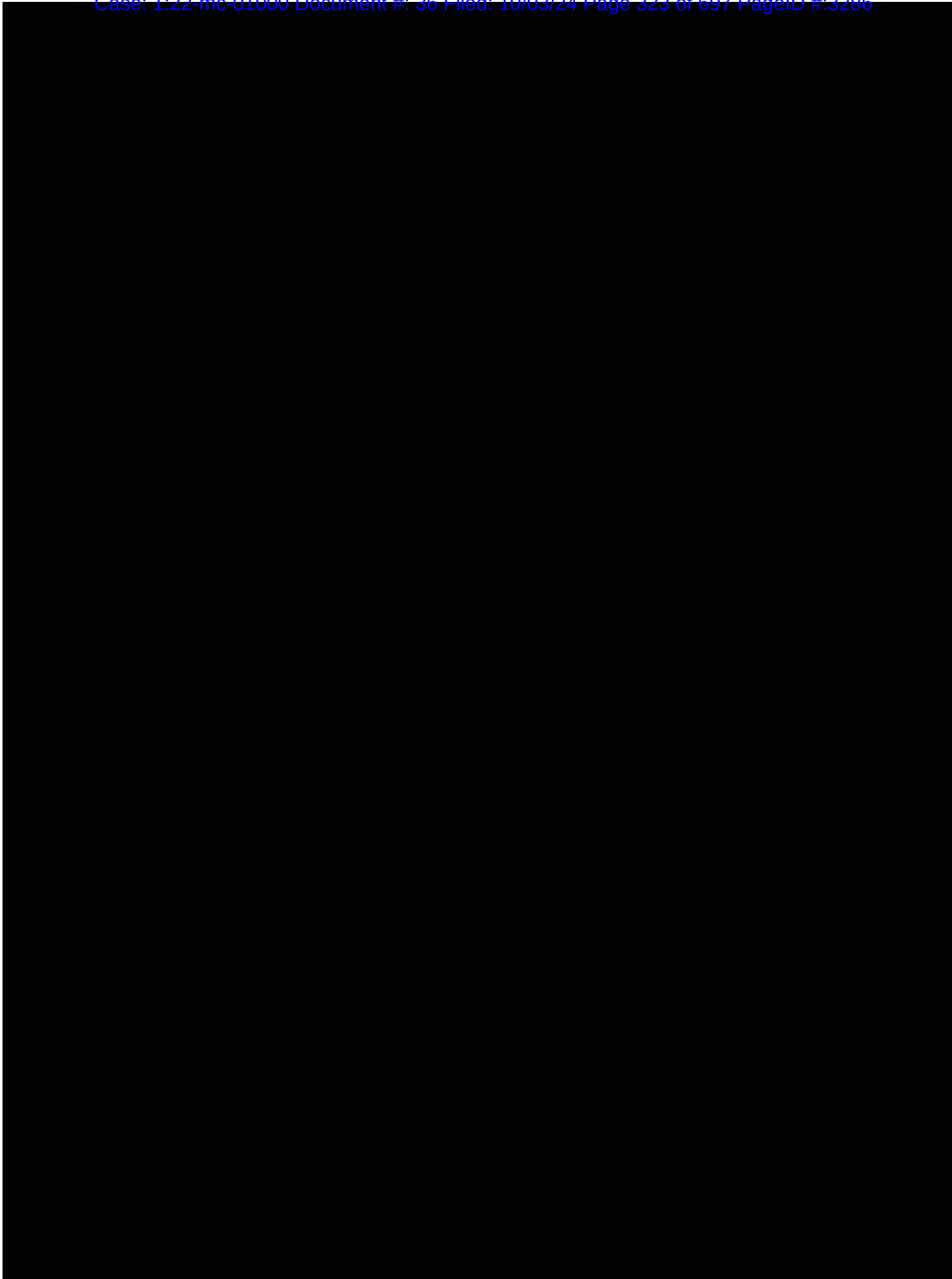


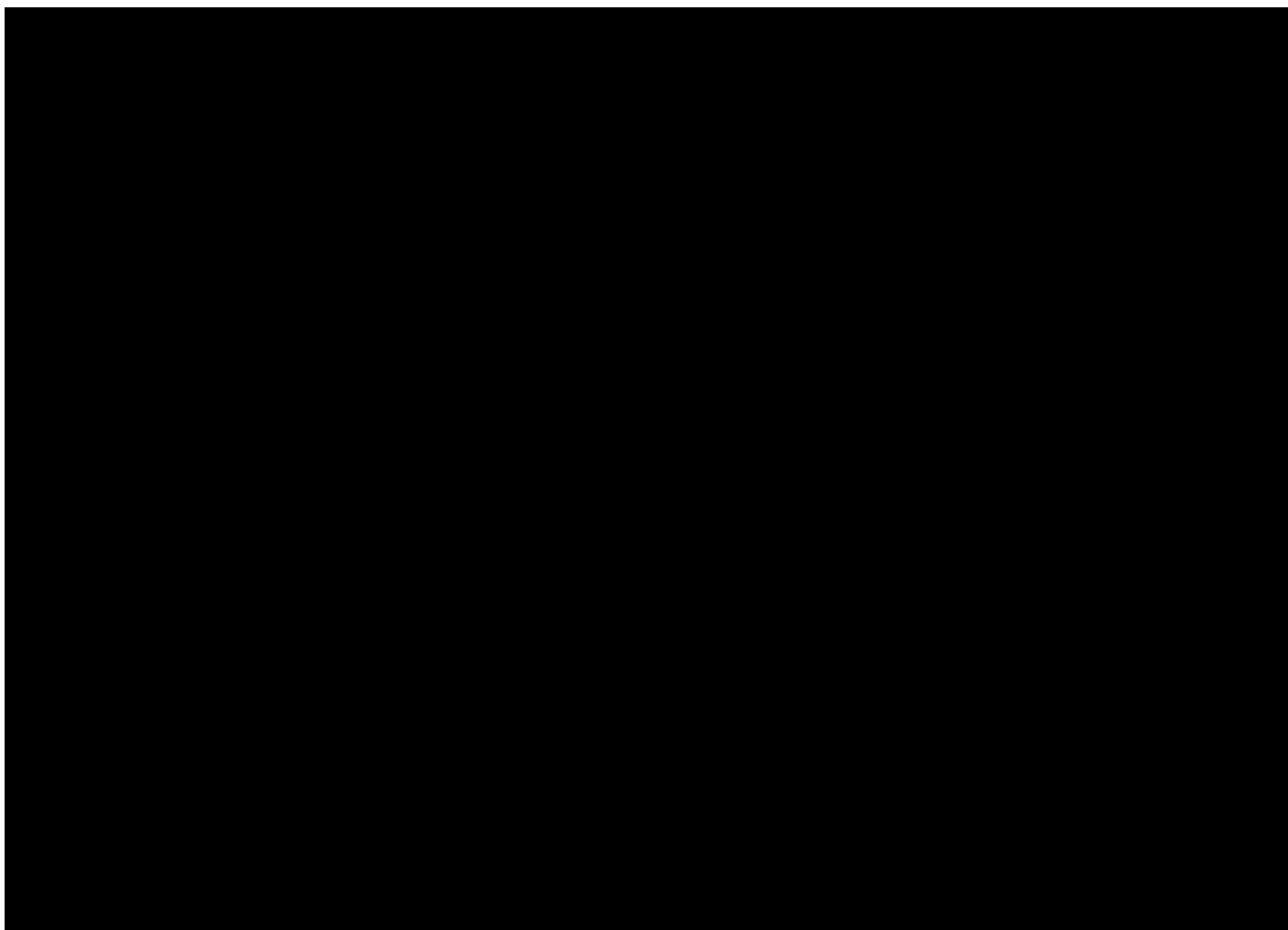


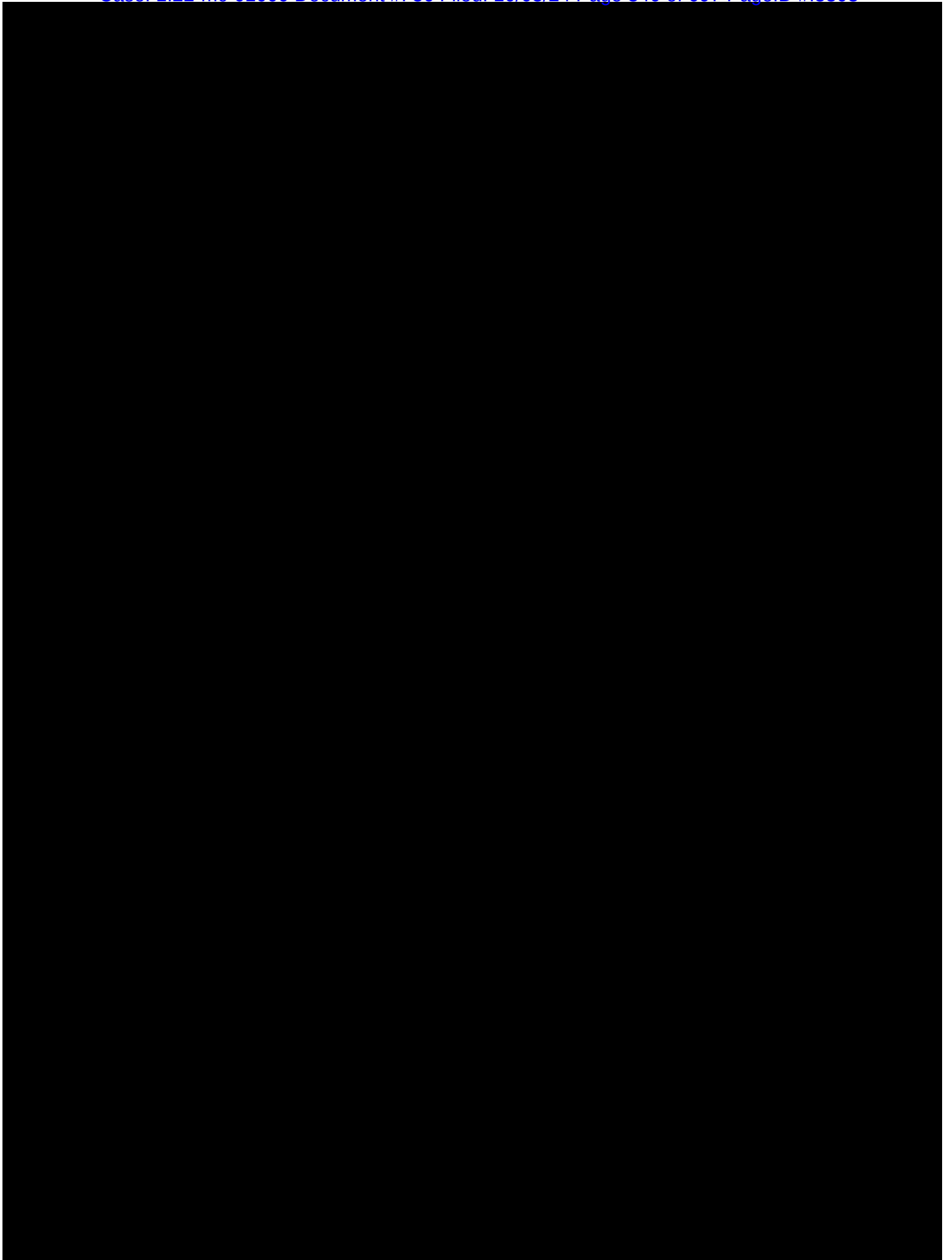
[REDACTED]

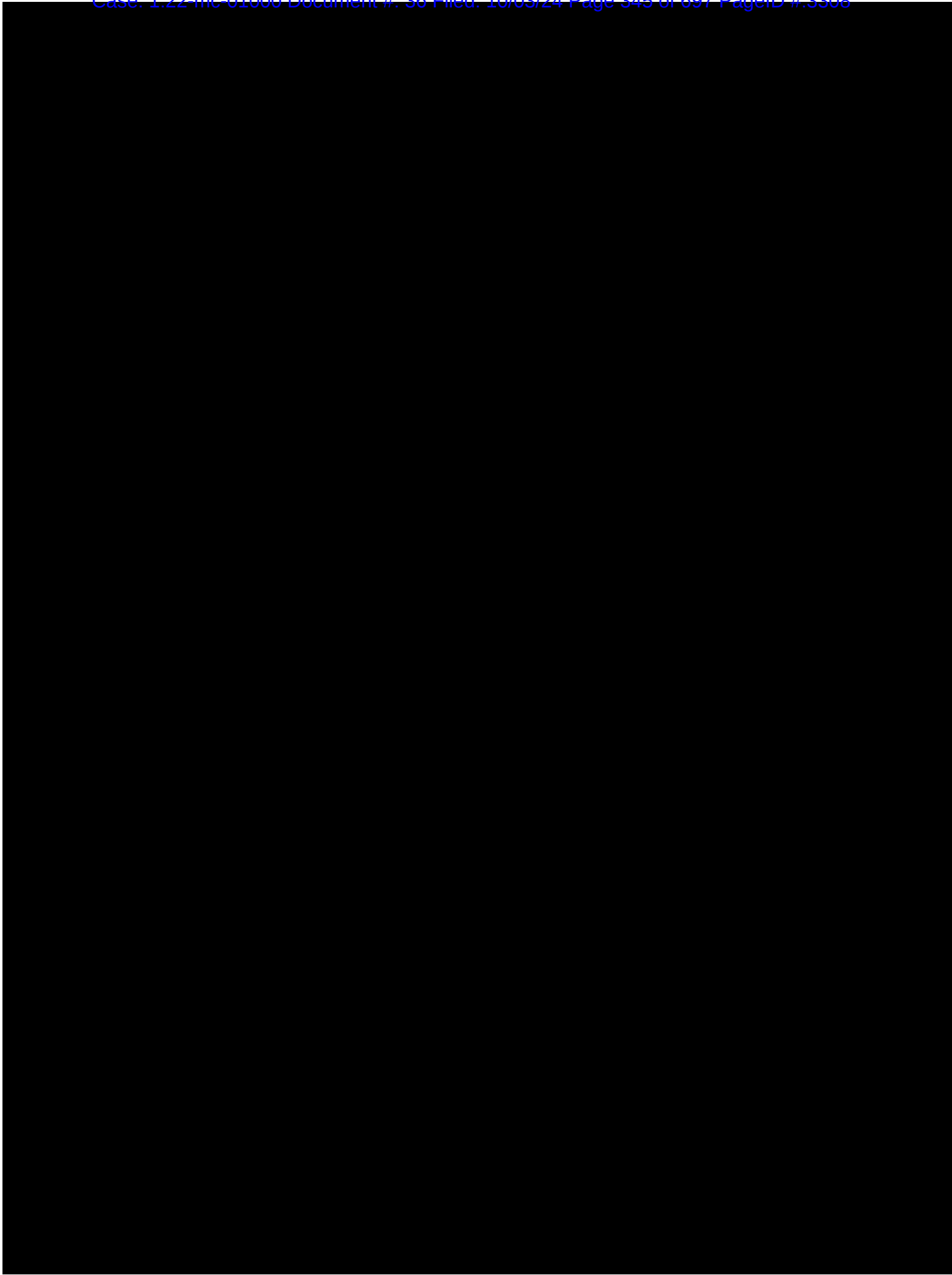
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	:	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	:	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	:	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	:	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	:	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

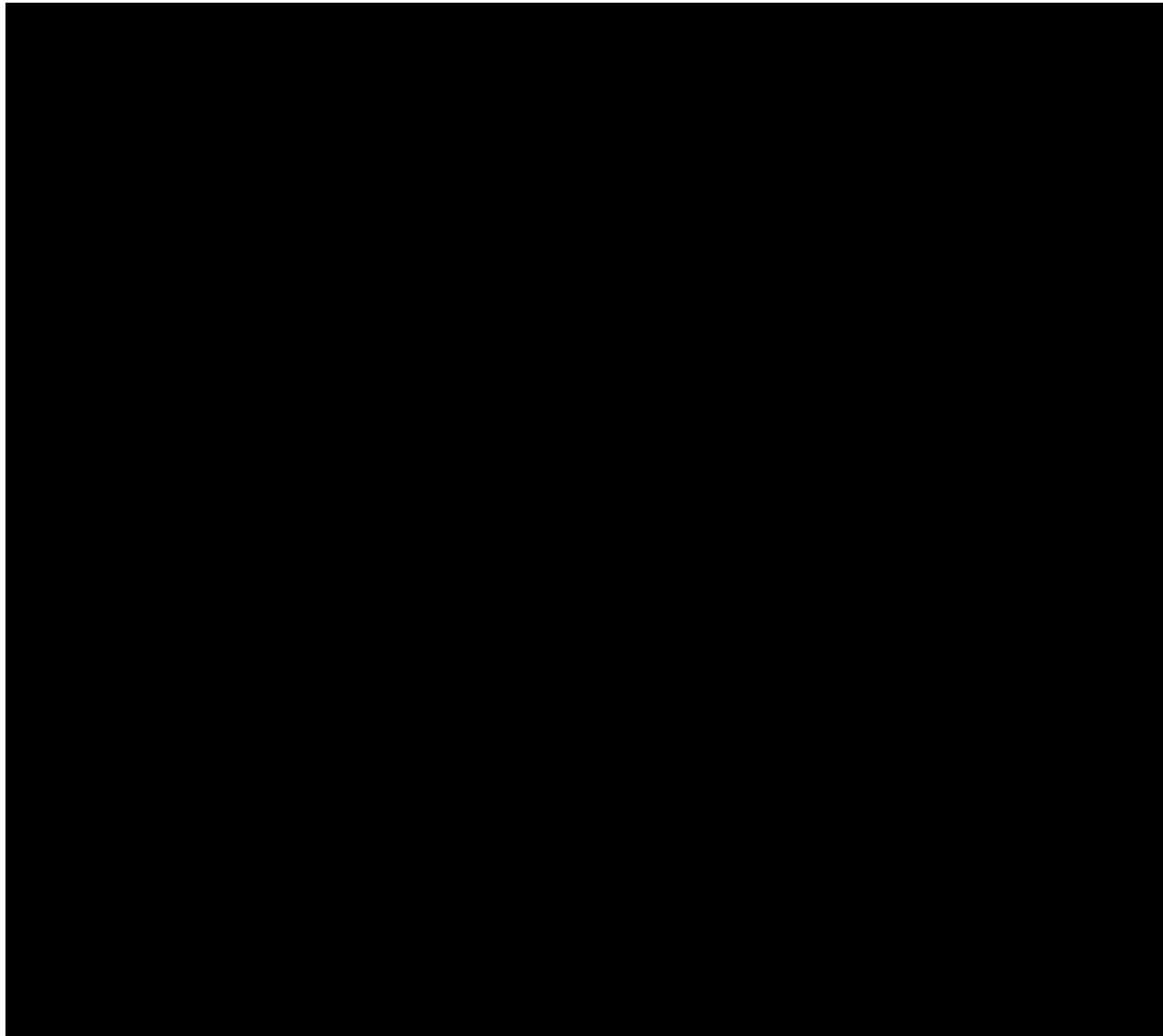


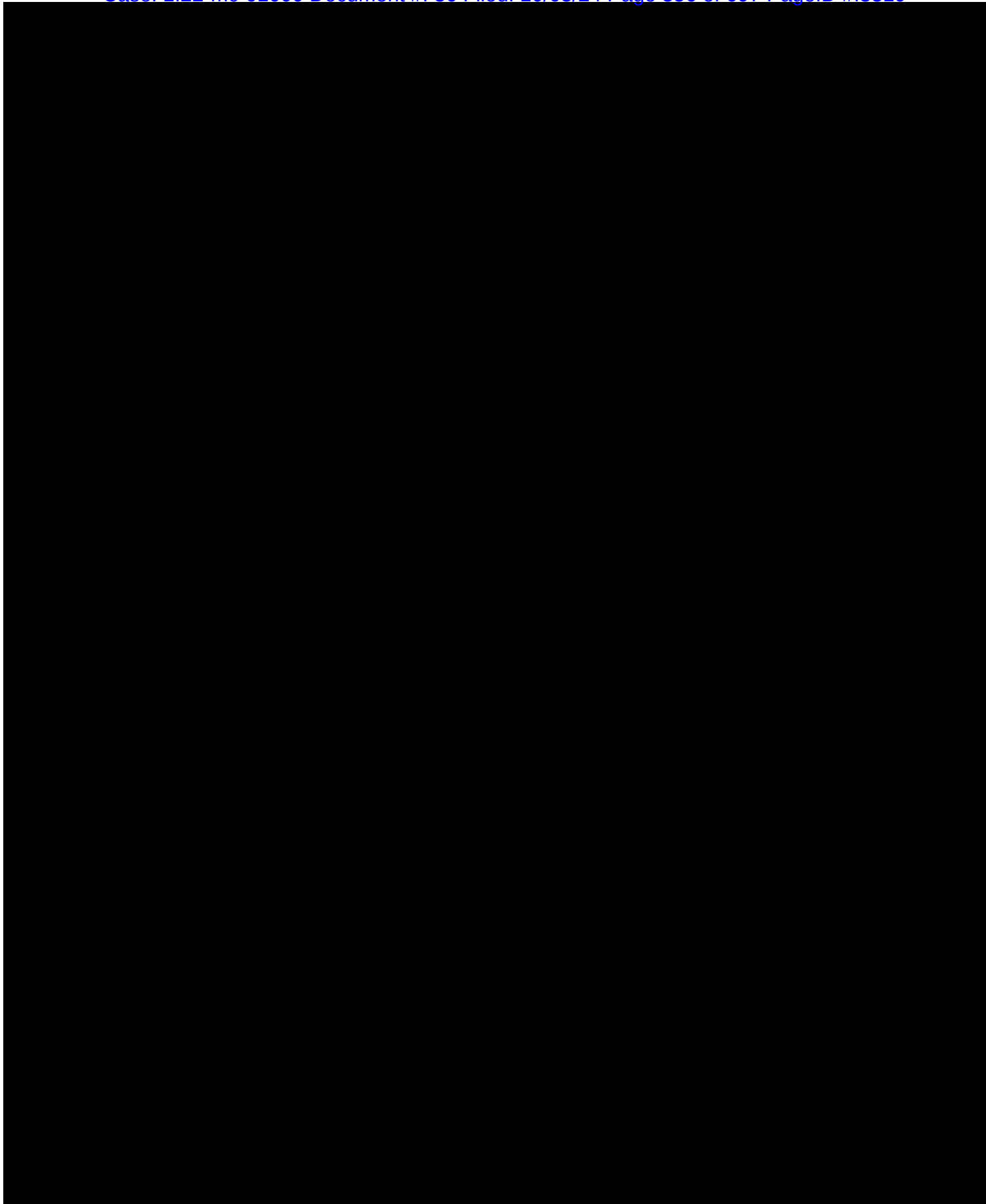


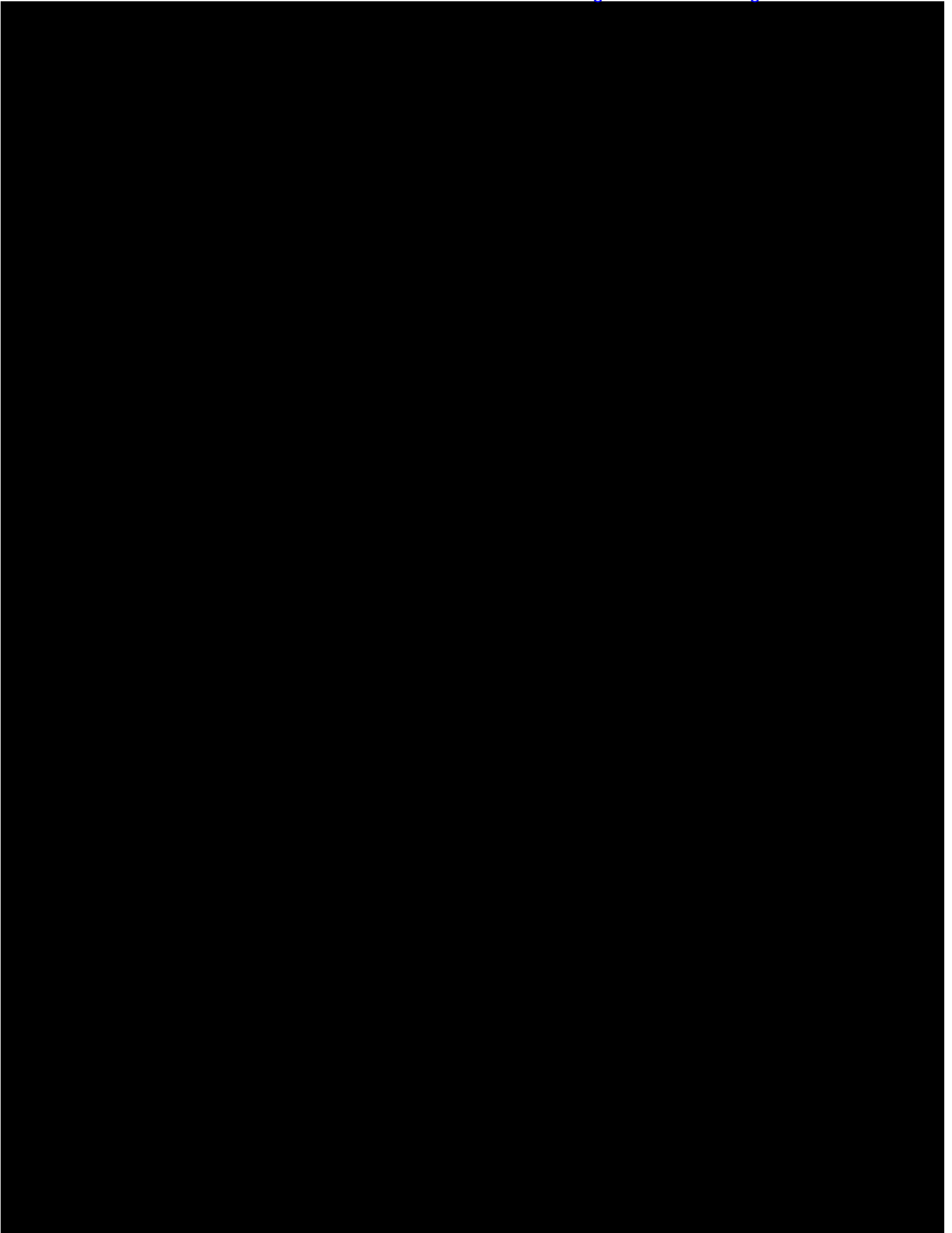


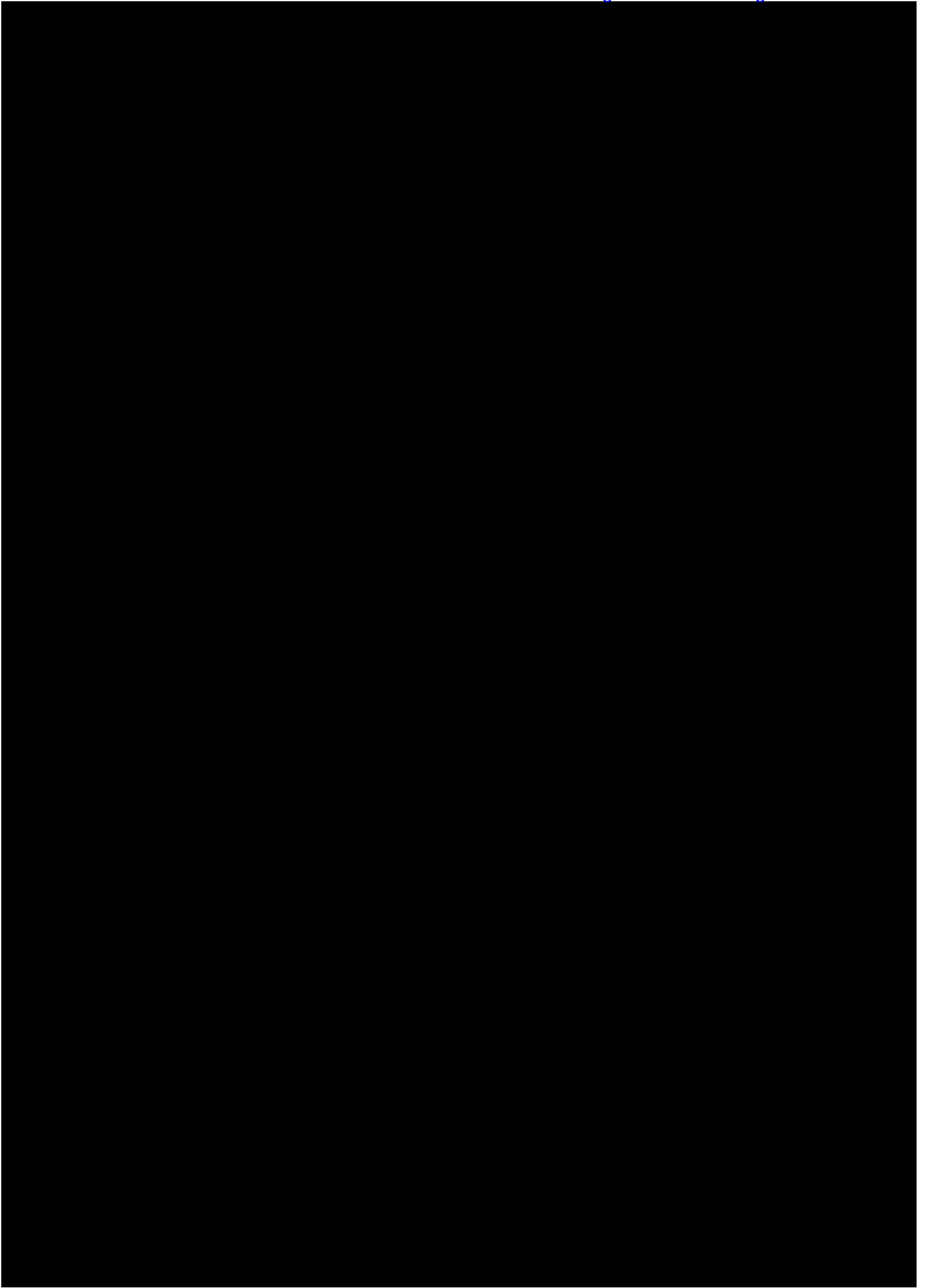


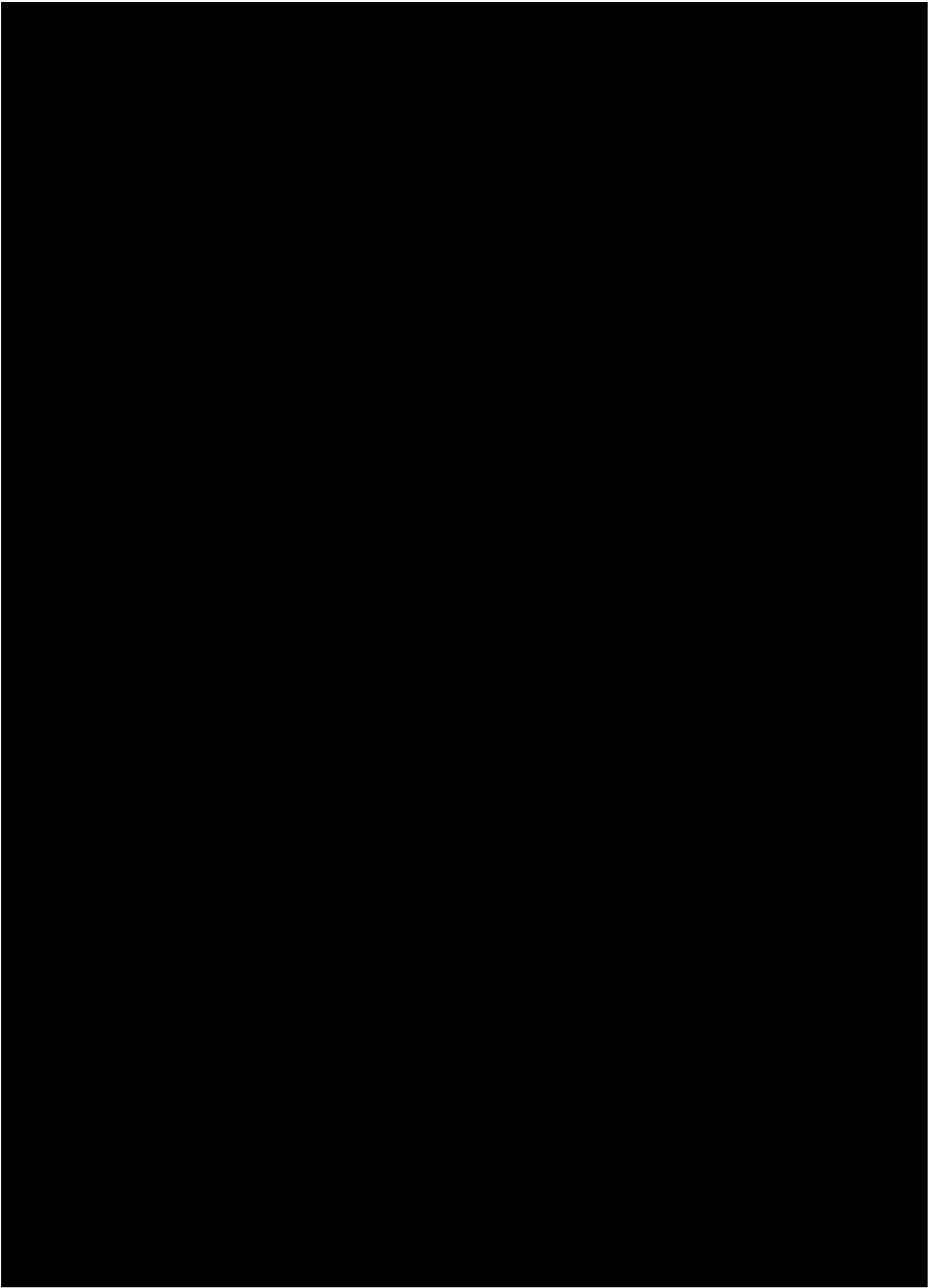


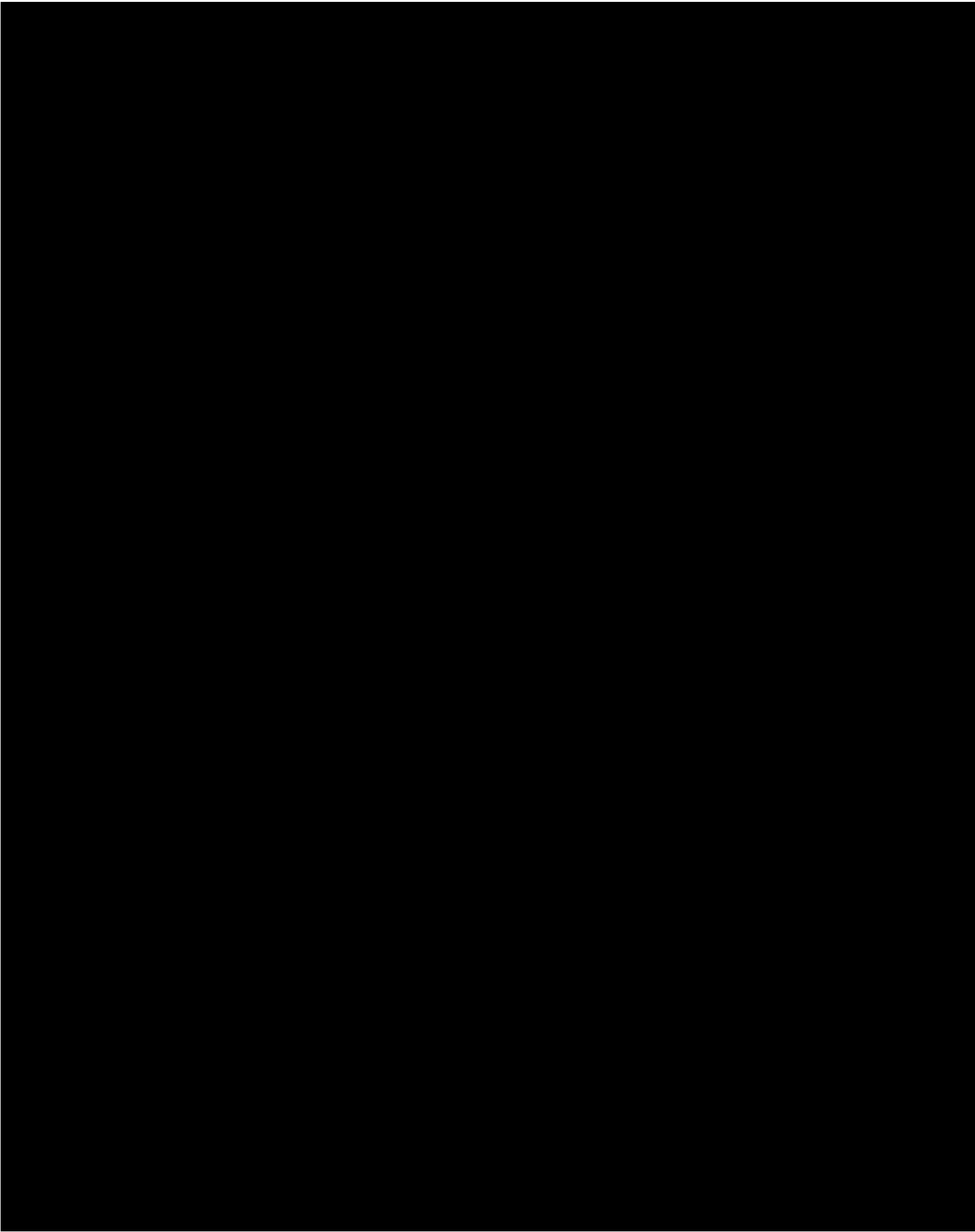


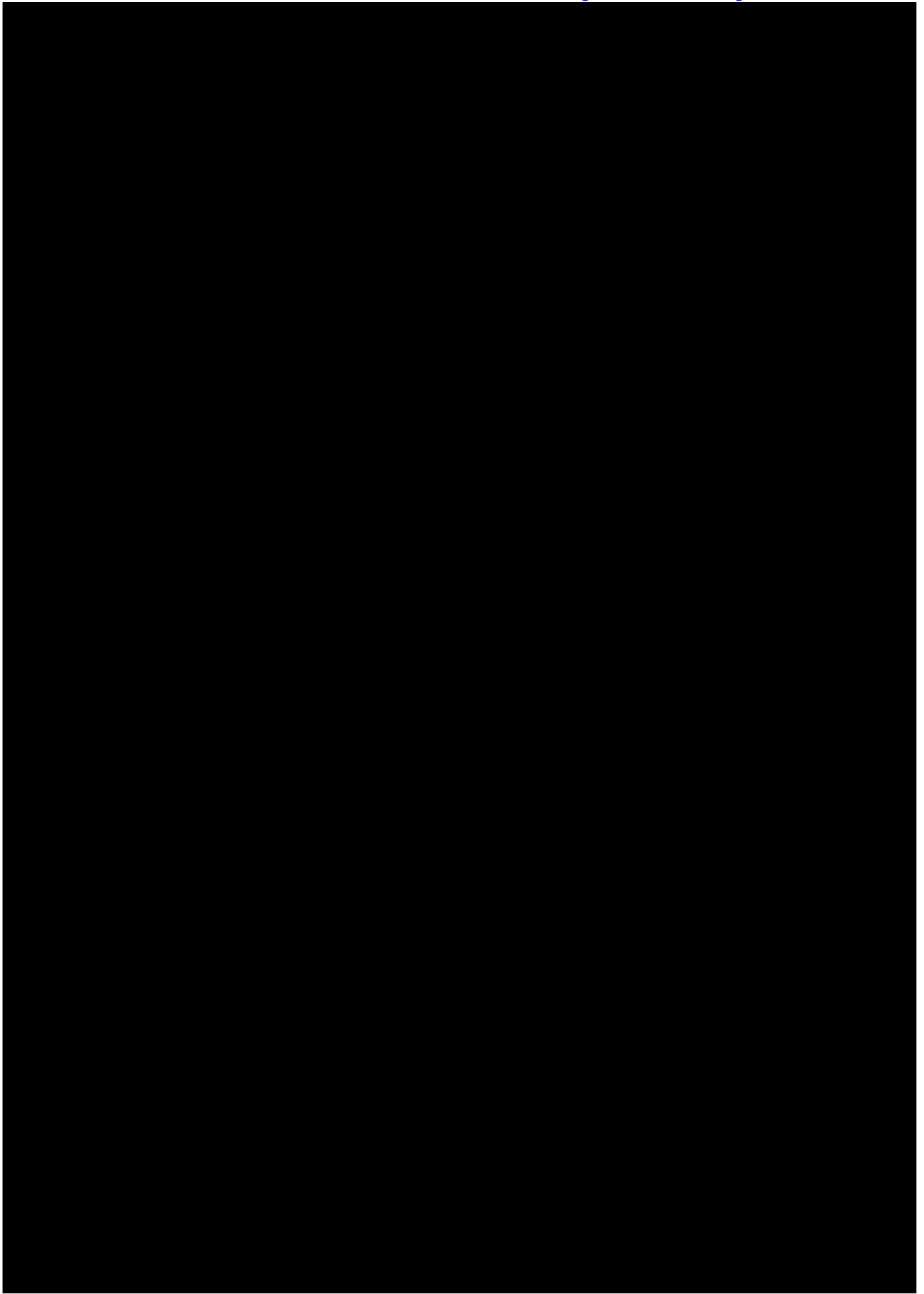


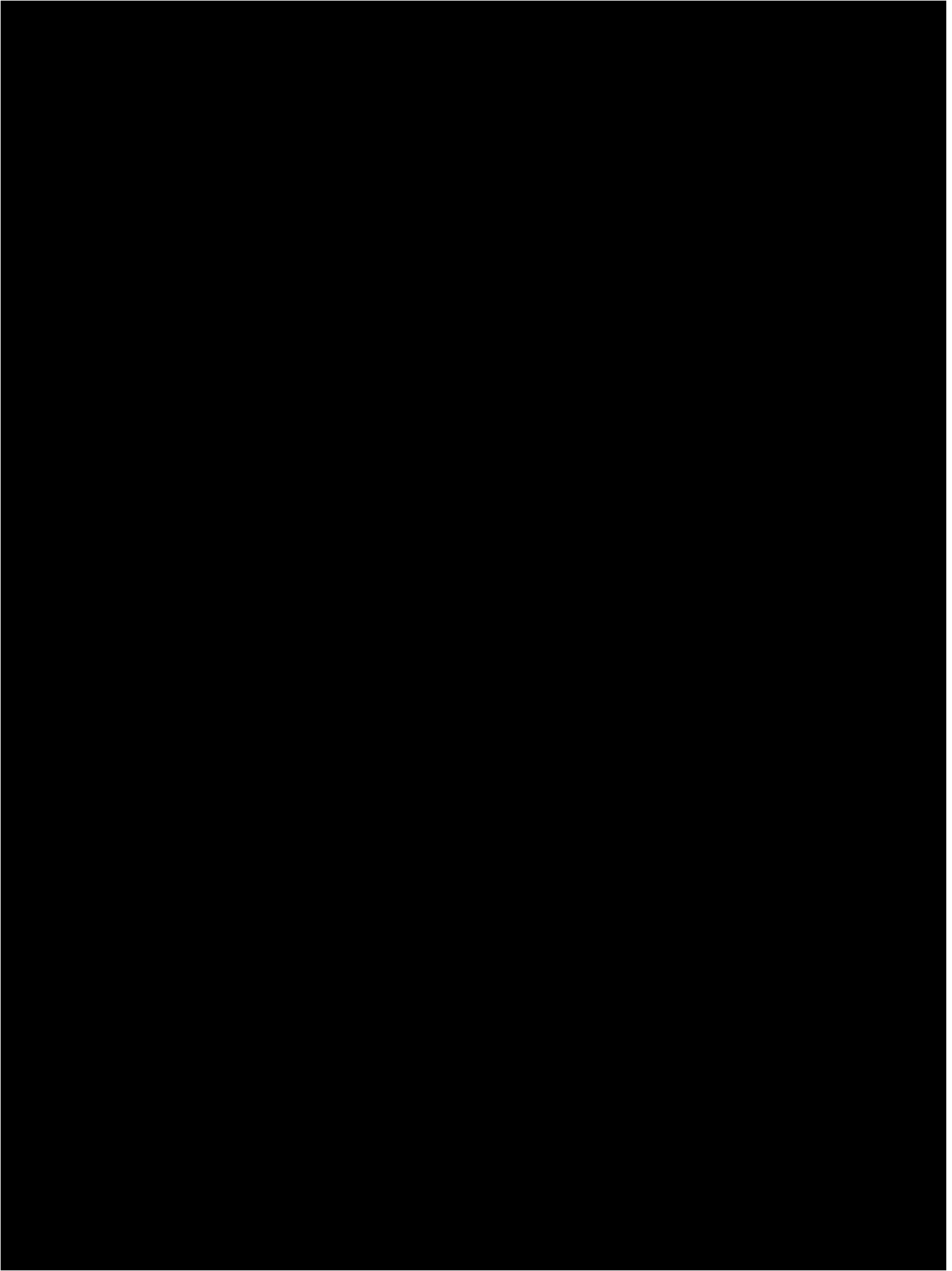


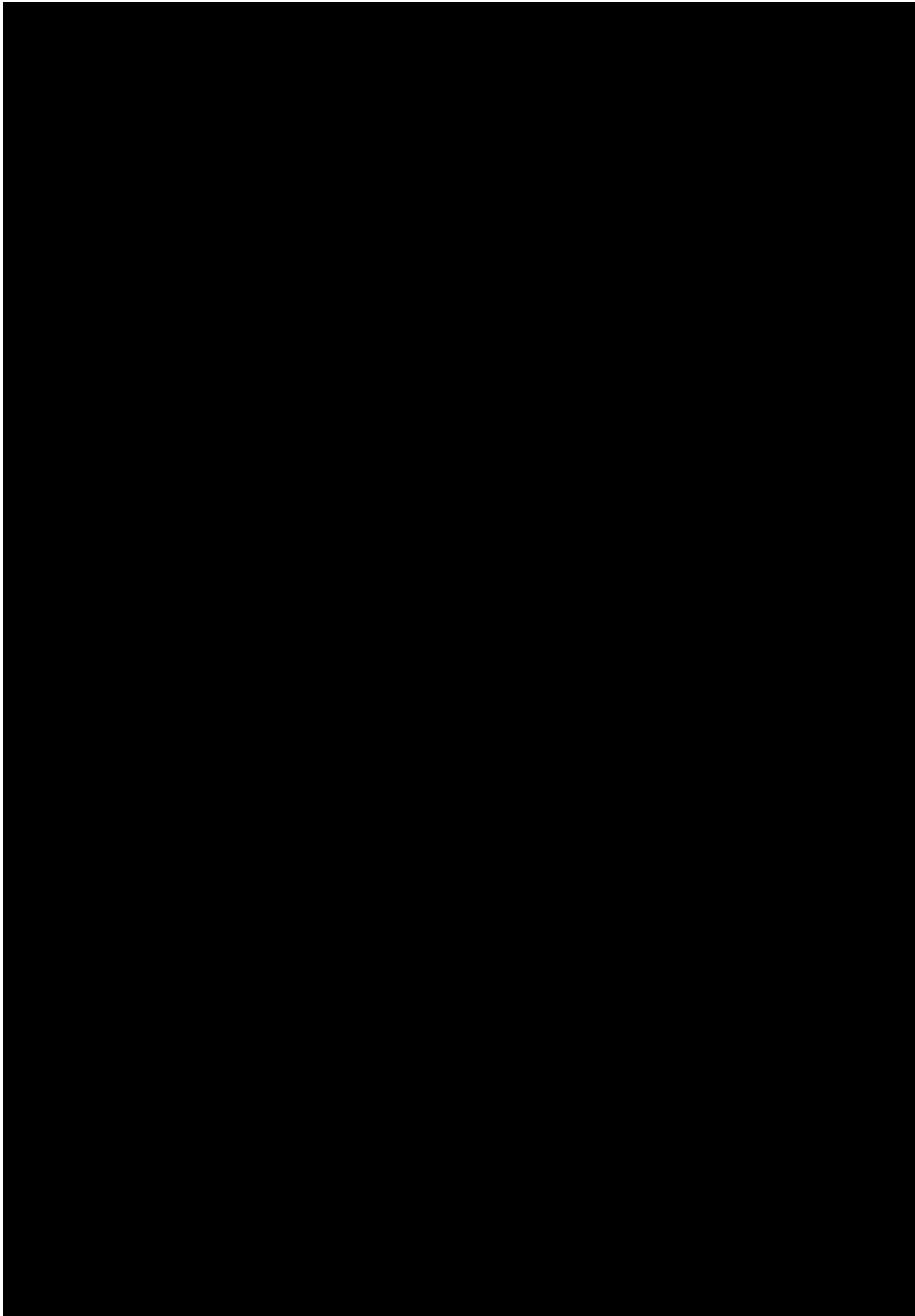












e

s

d

k

l

d

n

t

o

e

s

e

e

y

h

y

)

y

